Version 9.6

AT&T Global Network Client

Administrator's Guide

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of publication. However, information is subject to change.

Microsoft Public License

The Application uses Open Source Software that is licensed under the Microsoft Public License (the "License"). You may not use this file except in compliance with the License. You may obtain a copy of the License at http://dotnetzip.codeplex.com/license. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Notice 2
Microsoft Public License 2
Overview 10
Using this Document 10
Related Documents 10
Your Network Service 11
Remote Access Service 11
Managed Virtual Private Network Services 11
Supplementary Service Options 11
Extended Access 11
AT&T Global Network Client Firewall 11
Lightweight Policy Enforcement 12
Authentication Types 12
AT&T Authentication Server 13
RADIUS 13
Authentication Providers 13
LDAP/Digital Certificates 13
AT&T Global Network Client Overview 14
Preparing for Installation 15
System Requirements 15
Requirements for Installation & Use 16
Installation 17
AT&T Global Network Client Installation Packages 17
Obtaining the AT&T Global Network Client 18
Distribution 18
Local Installation 19
Group Policy Distribution 19
Upgrading Previous Releases 19
Selecting Your Language Support 20
Filter Driver Installation 20

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T T6 Client 21
Configuration 22
The Connection Sequence 22
Automatic Prompting for Configuration during Dial Connections 24
Advanced Configuration 26
Central Configuration 26
Profile Management 26
Login Properties 26
Profile Manager 27
Network Services 27
Servers 28
Preferences 29
Autostart 30
Post Connection Script 31
Programs 32
Timeouts 33
Connection Features 34
Persistent Connections 34
Configuration for AT&T Services (AT&T VPN or Business Internet Services) 34
User Preference 34
Persistent Connection Mode 35
Enabling Persistent Connections during Installation 35
VPN Mobility 36
Limitations 36
Configuration 37
Advanced Configuration 37
User Preference 39
AutoReconnect 39
Prevent Multi-Homing 40
Configuration 40

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

User Preference 40
AutoConnect Feature 40
Software Updates 41
Suppress Program Updates 41
User Permissions 41
Software Update Process 41
Automated Check for Updates 41
Manual Check for Updates 42
Feature Specific Updates 43
Uninstall 44
Local Uninstall 44
Uninstall 44
Remove Warning 47
Remote Uninstall 47
Command Line Uninstall 47
Customizations 48
Advanced Customizations Using Windows Installer 48
AT&T Global Network Client Features 48
Public Properties 50
Shortcuts 55
Common Windows Installer Properties 57
Using the Command Line to Customize Installation 57
Example Command Line Customizations 58
Creating a Windows Installer Transform 58
Tools to Create a Transform 59
Common Changes Customized via a Transform 59
Things That Must Be Avoided 60
Recommended Actions via a Transform 60
Adding Files 60
Updating Files 61

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Customizing Your Password Rules 61
Changing the Installation Directory 61
Changing the Application Name 61
Making the Transform Apply To Future Versions 61
Customization Using a config.xml File 62
Global Customizations (FastPath Replacement) 62
Trusted Domain Customization 62
Trusted Domain Configuration 63
Trusted Domain Customization Limitations 63
Client Profiles Customization 63
Client Profiles Configuration File 63
Other Commonly Requested Customizations 66
Network Login Option Customizations 67
Hide Options Button 67
Use Digital Certificates 67
Password Format 68
Other Network Login Options 68
Limiting Connections Per Operating System 69
Profile Customization Limitations 69
Controlling the AT&T Global Network Client Firewall 69
Network Awareness Customization 69
Defining Networks and Corresponding Actions 71
Approved Mobile Device Customization 73
Approved Connection Type Customization 73
Secondary Method of Customizing Network Login Options 73
Customizing Default Login Options 74
Customization Services 76
SDK Prioritization 76
Accessibility Features 77
Visual Display of Screen Element in Focus 77

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Keyboard Navigation 77
Extended Access 78
Extended Access and AT&T Business Internet Service (BIS) 78
Internet Extended Access Authentication Options 78
Extended Access and AT&T VPN Services (AT&T VPN Tunneling Services) 78
AT&T Lightweight Policy Enforcement 79
Asset Based Connection Prevention 79
Operating System 79
Application Monitoring 80
Types of Applications Monitored 80
Limitations 81
Lightweight Policy Enforcement Customization Examples 81
AT&T Global Network Client Firewall 87
Overview 87
OPSWAT Certified Firewall 87
Operating Modes 88
Default 88
Trusted Domains 88
User Controlled 88
Disabled 88
Firewall Settings Window 88
Managed VPN Access Control Lists 89
Limitations 90
AT&T VPN Services 91
Using Managed IPSec VPN Services 91
Local Resources 91
Sharing Local Resources 91
Registering VPN IP Address with Dynamic DNS 91
Encryption for IPSec VPN connections 92
Co-existence with Microsoft IPSec 92

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

NAT Traversal 92
Configuring UDP Encapsulation 92
Cisco Passwords 93
Using Managed SSL VPN Services 93
Network Layer Solution 93
Security/Authentication 93
Configuring the AT&T Global Network Client to Establish a VPN Connection through a Proxy 94
Importing a Proxy File for SSL connections 94
Proxy.ini File 94
proxy.ini Field Information: 95
Importing the Proxy.ini file 95
Switching to IPSec Over Dial Connections 96
Dynamically VPN Connect 96
IPv6 Support 97
IP version preference 98
IP version failover 98
OPSWAT Certified VPN 98
Integrating with Third Party Software 99
ThinkVantage® Access Connections™ 99
WireShark® and Microsoft Network Monitor 99
Help/Customer Support 100
Support Forum 100
Contact AT&T 100
Frequently Asked Administration Topics 101
Using Digital Certificates for Authentication 101
Using Mobile Monitoring Programs 101
Connecting Directly to a Mobile or Wi-Fi Network 101
Troubleshooting Installation 102
Appendix A: Central Configuration 103
Central Configuration Values 103

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T Administration Server Client Configuration Values 104
Additional Service Information 113
Appendix B: Supported Mobile Devices 114
AT&T Supported Mobile Devices 114
Mobility SDK Technology Use 119
Embedded Modules 120
Other Supported Mobile Devices 120
Appendix C: Third-Party Firewall Support 139
Network Firewalls 139
SMiX List 140
Personal/Client Firewalls 141
Dial Authentication 142
Disconnect warning 142
Software updates 142
SLA data collection 142
Configuration Updates 142
Appendix D: Using the Command Line Program 144
AT&T Client 144
Parameters: 144
AT&T Global Network Client Firewall 148
Appendix E: AT&T T6 Client 149
Corporate Networks 149
Operating Systems 149
Components of the T6 Client 149
System Tray Icon 149
Software Updates 150
Tray Icon Menu 150
Index 155

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Overview

The AT&T Global Network Client is a program that enables your Windows computer to easily connect to the Internet or your company's private network.

Using this Document

This document is intended for IT professionals that are deploying the AT&T Global Network Client to their employees, or IT professionals that wish to gain a better understanding of the administration of AT&T remote access services.

The reader is assumed to be an IT administrator with a technical knowledge of Microsoft Windows® and computer networking and is referred to in this document as the customer account administrator.

Related Documents

AT&T Global Network Client User's Guide

ftp://ftp.attglobal.net/pub/client/win32/9.6.0/usersguide.pdf

AT&T Domain Login Guide

ftp://ftp.attglobal.net/pub/client/win32/9.6.0/domainlogonguide.pdf

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Your Network Service

AT&T enterprise mobility consists of a portfolio of managed services for remote access, VPN, and endpoint security. AT&T provides the service and the support for your managed network service; however, account administration and user configuration is controlled by you, the Customer Account Administrator, for all users associated with your account. AT&T provides you with central tools to manage and configure your individual account and user experience, storing the settings in the AT&T administration server. The AT&T Global Network Client interfaces with the AT&T administration server to receive configuration information.

Your administration of the AT&T Global Network Client requires basic knowledge of the features of your network service.

Remote Access Service

Remote Access Service (RAS) provides a remote computer with basic IP connectivity to the Internet.

Managed Virtual Private Network Services

Managed Virtual Private Network (VPN) Services provide a remote computer with connectivity to a private Intranet.

AT&T IP-VPN Services use the AT&T Global Network Client to perform all aspects of the network service, including establishing and maintaining the VPN connection.

Supplementary Service Options

Extended Access

Extended Access is an AT&T service feature that allows remote users to access the network through local points of presence that are owned and managed by another Internet Service Provider (ISP). Extended Access provides local access in countries where AT&T does not have points of presence. There is an hourly access charge for the use of Extended Access – the amount of which is based on the region in which the Extended Access takes place.

AT&T Global Network Client Firewall

The AT&T Global Network Client Firewall is a component of the AT&T Global Network Client which provides basic firewall capabilities. The AT&T Global Network Client Firewall uses the Windows firewall engine for the firewall and fencing.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Lightweight Policy Enforcement

AT&T Lightweight Policy Enforcement (LPE) is an optional service which performs basic application monitoring and can be customized by the Customer Account Administrator at installation time.

Authentication Types

AT&T allows each customer to select the type of authentication engine implemented for users of their account.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T Authentication Server

Many customers allow AT&T to manage their user authentication via the AT&T authentication server (a.k.a. AT&T Service Manager). You, as the Customer Account Administrator, can define and administer the users within your account using central tools.

RADIUS

It may be possible for the AT&T authentication server to interface with your RADIUS server for user authentication. User accounts are defined in the AT&T authentication server for administration and all authentication requests proxy to your RADIUS server via the AT&T authentication server for validation.

Authentication Providers

Several authentication providers are supported with the AT&T Global Network Client. Both hardware token as well as software token solutions are supported. For software solutions, the applicable software must be installed on the workstation to enable the token-based authentication. RSA SecurID®[1], SafeWord, SoftToken, CryptoCard and Defender are all supported via RADIUS.

LDAP/Digital Certificates

AT&T offers the use of Entrust and Microsoft digital certificates to authenticate users for Internet and AT&T IP-VPN services.

[1] EMC2, EMC, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. Aladdin, SafeWord, PremierAccess, RemoteAccess, and SecureWire are trademarks of Aladdin.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T Global Network Client Overview

The AT&T Global Network Client is software that allows Windows computers to easily access the Internet and your company's private network from many locations around the world. It provides a simple, powerful interface designed to automatically detect and connect over mobile, Wi-Fi, broadband, dial, and ISDN networks. It also is designed to provide security policy enforcement, offline hotspot and dial directory browsing, detailed connection history, and in-depth diagnostic logging.

The AT&T Global Network Client is available in two installation packages. The AT&T Global Network Client installation package includes all required and optional features and can be used for the majority of installations. The AT&T Global Network Client for Export installation package does not contain VPN encryption software for use in countries which restrict the import of such technology. More information about the AT&T Global Network Client installation packages can be found in the Installation Chapter of this document.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Preparing for Installation

System Requirements

The AT&T Global Network Client and its components are supported* on the following operating systems and hardware. (The AT&T Global Network Client may function properly on other operating systems and lesser hardware, but it is not formally tested or supported):

Operating System	Software	Hardware
Windows® Vista Windows® 7 Windows® 8/Windows 8.1 ***Administrator Rights Required***: The user must have administrator rights when the installation is executed.	Windows Installer 3.5 or later .Net Framework 4.0 or 4.5 MSXML 3 or 4	IBM PC or 100% compatible 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor 2 MB RAM or higher recommended 250 MB free disk space Dial connection: 14,400 modem recognized & configured by Windows Wi-Fi connection: wireless adapter that adheres to NDIS 5 specifications and tested by AT&T Mobile connection: PC Mobility Card

*The following limitations apply to support for Windows 8:

- As with previous releases, drivers for embedded devices are provided by the laptop manufacturer (check for availability before upgrading)
- When connecting to AT&T Wi-Fi and certain Partner Hot Spots, the operating system may unnecessarily display the browser

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Requirements for Installation & Use

Before starting the AT&T Global Network Client installation and setup, verify you have the information required in the following checklist. If you are missing any information, please contact your Customer Account Administrator.

- Administrator rights to install or upgrade
- Your Windows install media (CD or installed MSI files) may be required.
- Hardware/Equipment necessary to establish basic network connectivity. For example, an existing Internet connection via cable or DSL, Wi-Fi, Mobile modem/card, ISDN terminal adapter, or a Dial modem & phone line.

For connections which require credentials:

- Account
- User ID
- Password, passcode, or PIN and token

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Installation

The AT&T Global Network Client installation is packaged using Microsoft Windows Installer and InstallShield® 2013[2] and can be installed and updated locally. Terminology specific to Windows Installer is used in this document and a basic knowledge of Windows Installer is useful when administrating the installation of the AT&T Global Network Client package. More information about Windows Installer can be found by consulting the "Roadmap to Windows Installer Documentation" at http://msdn.microsoft.com/en-us/library/aa371366(VS.85).aspx

AT&T Global Network Client Installation Packages

The AT&T Global Network Client is available in two installation packages. The AT&T Global Network Client installation package should be used for the majority of installations. The AT&T Global Network Client for Export installation package is available for use in countries that prohibit the import of VPN encryption technology.

An overview of the installation package to be used with each service is shown in the table below.

	AT&T Global Network Client	AT&T Global Network Client for Export
Remote Access Services	✓	✓
AT&T VPN Services	✓	
Extended Access	✓	✓
AT&T Global Network Client Firewall	✓	✓
Lightweight Policy Enforcement	✓	✓
Mobile Drivers	✓	

Figure 1: AT&T Global Network Client Installation Packages

[2] Flexera Software, AdminStudio, FlexNet Connect, InstallShield, and InstallShield Professional are registered trademarks or trademarks of Flexera Software LLC in the United States of America and/or other countries.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Obtaining the AT&T Global Network Client

The AT&T Global Network Client is distributed through a public Internet download. If you have previously installed from a private FTP/Intranet download location you may be using a custom version of the AT&T Client; contact your Customer Account Administrator to request an updated version.

Users of Custom Versions: Do not manually download new releases. Contact your AT&T Account Representative to request an updated customversion.

Two different installation packages are available for download. The single file executable (.exe) installation package is used for most user based installations. The single file executable has the benefit of detecting previous AT&T Global Network Client installations and automatically performing the correct upgrade. The compressed single file MSI (.msi) installation package is useful if you wish to use a software distribution technology to push software updates out to your users.

Package	Downloads
AT&T Global Network Client	ftp://ftp.attglobal.net/pub/client/win32/9.6.0/agnc.exe ftp://ftp.attglobal.net/pub/client/win32/9.6.0/msi/agnc.msi
AT&T Global Network Client for Export	ftp://ftp.attglobal.net/pub/client/win32/9.6.0/agnc_export.exe ftp://ftp.attglobal.net/pub/client/win32/9.6.0/msi/agnc_export.msi

Figure 2: Download Location Table

Distribution

The AT&T Global Network Client is distributed for local installation. Customization and pre-installation configuration are supported. Microsoft Windows Administrator rights are required when the AT&T Global Network Client is installed.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Local Installation

A local installation is initiated by the user on the target machine by executing one of the AT&T Global Network Client installation packages.

Administrator Rights Required:

The user must have Microsoft Windows Administrator rights/privileges when the installation is

Group Policy Distribution

When installing the AT&T Global Network Client using an Active Directory Group Policy you must define a new object in your Group Policy manager and define the Software Installation Package with the full network path to the installation files, not the local path to the files. *The installation files must be copied to the local machine to do the installation.*

Upgrading Previous Releases

If you already have the AT&T Global Network Client (version 7 or later) installed on your workstation, the installation can perform an upgrade to version 9.x. During the upgrade, the previous AT&T Global Network Client will be uninstalled, the workstation may be rebooted, and then the new AT&T Global Network Client will be installed. Administrators can suppress the reboot after the previous AT&T Global Network Client has been uninstalled by setting the installation property "SUPPRESS_UPGRADE_REBOOT=1" for the installation package but this feature is not recommended and will require detailed testing on your part prior to selection. For more information, refer to the chapter titledAdvanced Customizations Using Windows Installer."

As part of the upgrade process, the user's data and AT&T Global Network Client customizations will be preserved whenever possible. This is accomplished by renaming, then restoring the user's data directory and the custom data directory. Installation package customizations, such as a custom desktop icon, will not be preserved. More information about customizations can be found in the Customizations chapter of this guide.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Selecting Your Language Support

The AT&T Global Network Client automatically installs support for running in English, French, German, and Spanish. If the installation is being performed on a Japanese version of the operating system, the installation will also install support for running in Japanese[3].

Installing the files necessary to support English is required. Support for other languages is configurable using the Custom installation path.

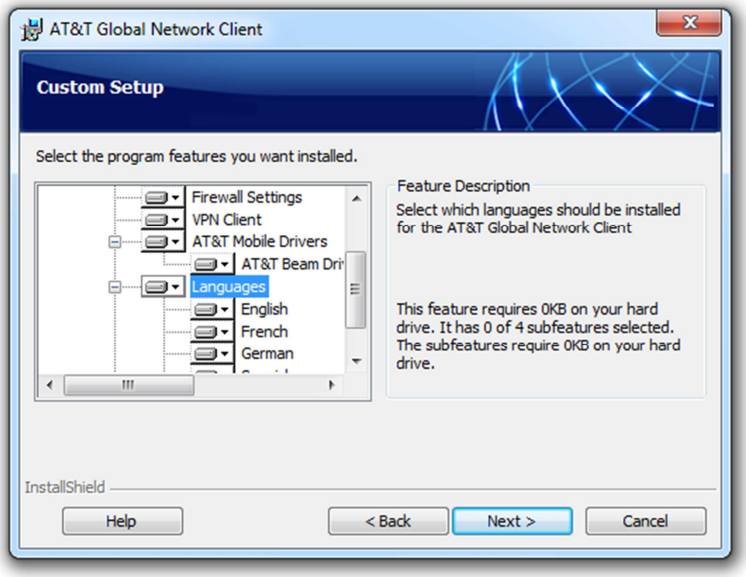


Figure 3: Select Your Language

The default language for the installation dialogs is English. To display the installation dialogs in French, German, Japanese or Spanish, or to automatically configure the languages installed for use by the AT&T Global Network Client, an installation Transform can be used. For more information on customizing the AT&T Global Network Client installation program, see the section titled Advanced Customizations Using Windows Installer

Filter Driver Installation

If a workstation has several filter drivers installed, such as if it has multiple VPN client installed, the AT&T Global Network Client installation may reach the default maximum number of filter drivers allowed, which would prevent installation of the client. The installation program will attempt to automatically prevent a driver installation error when installing the AT&T Global Network Filter Driver on Windows 7 and later. Upon detection of the error, the installation program is designed to increase the MaxNumFilters key by 1. It will then continue with the installation. The installation program will continue incrementing the MaxNumFilters until it is able to complete the installation.

[3] Japanese is only supported if installed on a Japanese version of the Microsoft Windows Operating System.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T T6 Client

The AT&T T6 Client provides support for IPv6. IPv6 is designed to succeed IPv4, the current version of Internet Protocol. The AT&T Global Network Client does not automatically install the AT&T T6 client. Use the Custom installation path to install the AT&T T6 client.

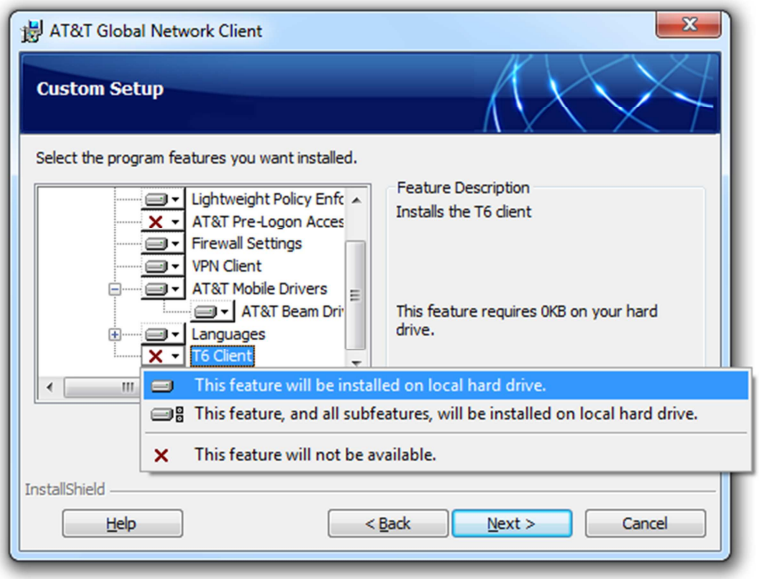


Figure 4: Install T6

For a complete description of the AT&T T6 Client please see Appendix E.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Configuration

Most users are able to establish a connection with no manual configuration prior to their first connection attempt, benefitting from the AT&T Global Network centralized administration and the AT&T Global Network Client automatic connection feature.

AT&T Global Network Client basic configuration is achieved through automatic prompting; advanced configuration is performed using central configuration settings or manually using the **Login Properties**.

The Connection Sequence

The AT&T Global Network Client attempts to connect using each of the available connectivity methods in the order they are shown on the main window.

Figure 5: Connection Sequence

The Dial connection type is not available and is not shown by default. It can be added if needed at install time using the SHOW_DIAL Public Property. End users can enable the Dial connection type by selecting 'Show Dial Connection' from the Settings menu.

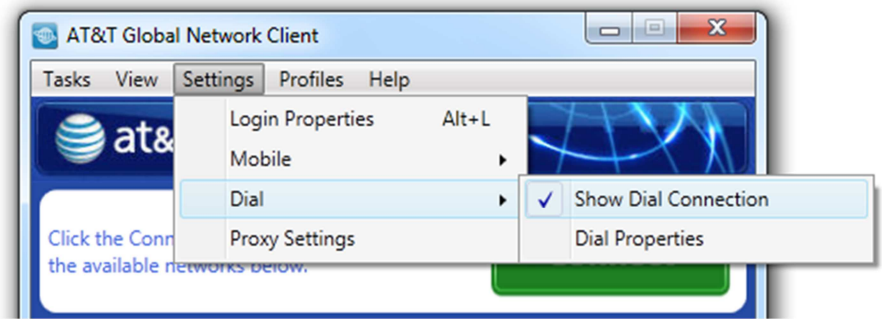


Figure 6: Show Dial Connection Menu

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Figure 7: Main Window with Dial Connection Shown

If a connectivity type is unavailable, the panel for that connectivity type will be disabled and will appear grayed out.

Figure 8: Connection Panel with Unavailable Connection Methods

If you would prefer to select a specific connectivity method to use for the connection attempt, click on the smaller green **Connect** button beneath the method desired, e.g. Wi-Fi.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Automatic Prompting for Configuration during Dial Connections

After you click **Connect** on the **Main Window**, the AT&T Global Network Client will prompt you for information required for a connection.

For dial connections, the **Browse Dial Directory** window will prompt you to select a phone number using your location information.

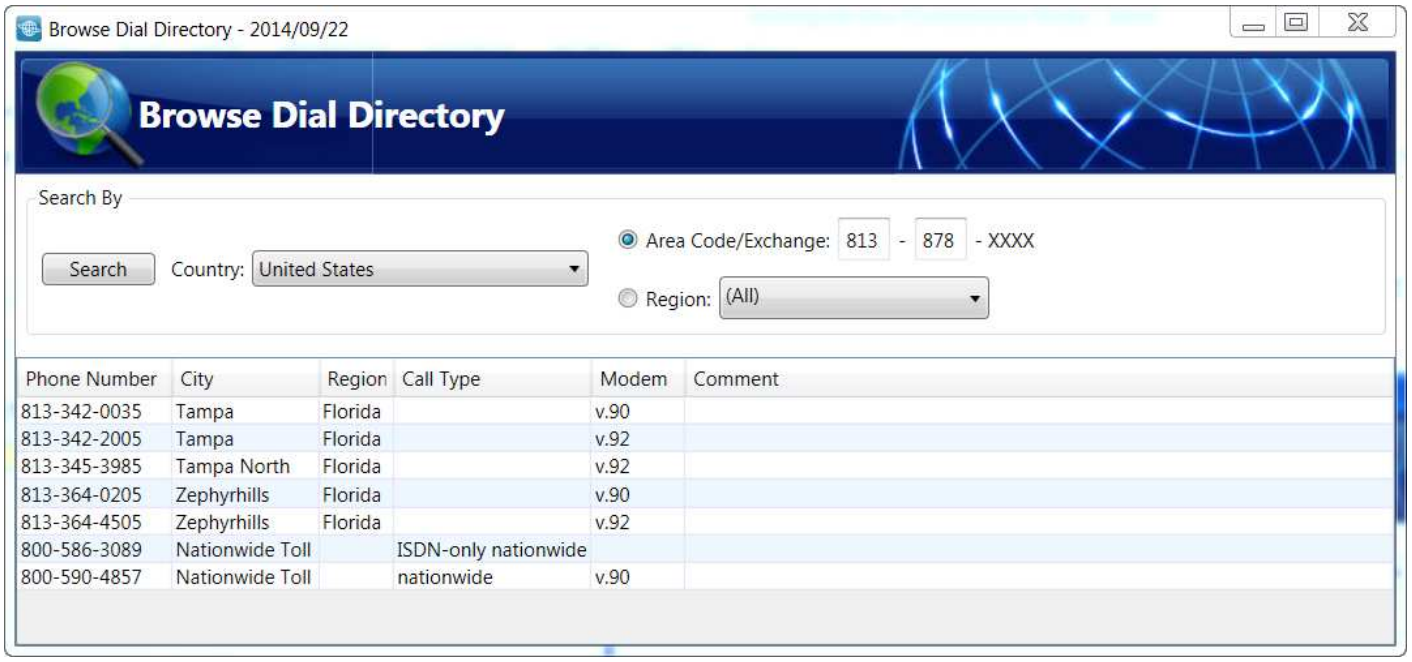

Browse Dial Directory - 2014/09/22
Browse Dial Directory
Search By
Search
Country: United States
Area Code/Exchange: 813 - 878 - XXXX
Region: (All)
Phone Number City Region Call Type Modem Comment
813-342-0035 Tampa Florida v.90
813-342-2005 Tampa Florida v.92
813-345-3985 Tampa North Florida v.92
813-364-0205 Zephyrhills Florida v.90
813-364-4505 Zephyrhills Florida v.92
800-586-3089 Nationwide Toll ISDN-only nationwide
800-590-4857 Nationwide Toll nationwide v.90

Figure 9: Browse Dial Directory

Select your country using the Country drop down list. You can then find nearby phone numbers either by entering the area code and exchange of the location from which you are calling, or by browsing your current region. Change the modem by selecting a modem using the **Connect using** drop down list. Verify the information for **Dial Prefix** and **Number to dial**. Click **OK** to continue.

You may also be prompted to supply your **Network Login** credentials (**Account, User ID** and **Password**) if you have not entered them previously.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Figure 10: Network Login Window

Once entered, your Account and User ID will automatically be stored for future connections. Your Password will be stored only if you click the checkbox next to Save Password. Customer Account Administrators can customize the AT&T Global Network Client so the Save Password option is not available. Refer to the chapter on Customizations on page 48 of this guide for additional information on hiding the **Save Password** option. Click **change…** to change your password. Click **OK** to continue.

Hardware Token Users: If you are using an authentication type which requires a PIN and token, enter your PIN immediately followed by the current token in the Password field.

Figure 11: Network Login Window – PIN and Token

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Advanced Configuration

Central Configuration

Central Configuration Simplifies Client Administration: Review all centrally configured values prior to distribution of the AT&T Global Network

The AT&T Global Network Client interfaces with the AT&T administration server to retrieve values set by you, the Customer Account Administrator.

Configuration of the values can be done by your AT&T representative or by you, via an AT&T provided administration tool. Refer to Appendix A on page 103 of this guide for additional information on central configuration.

It is recommended that you review the list of values supported by the AT&T Administration Server in Appendix A on page 103 of this guide and set values prior to the distribution of the AT&T Global Network Client to your users.

Profile Management

AT&T Global Network Client profiles store user information. A profile includes:

- Account
- User ID
- Advanced Login Properties (Service, WINS, DNS, Domain Suffix, Windows Login)
- Service

Most users connect with the same information a majority of the time and will only require one profile.

Users that connect with different user IDs may want to define profiles for their common user combinations to easily switch between them. AT&T Global Network Client profiles can be assigned common names to help you remember when to use them, for example, 'My Internet Profile' or 'VPN Servers – Germany'.

Login Properties

To access **Login Properties** click the **Settings** Menu > **Login properties** on the main window of the AT&T Global Network Client.

The AT&T Global Network Client - **Login Properties** window allows you to configure the settings and properties for your current connection. It is recommended you use the default values and values defined in the AT&T administration server.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

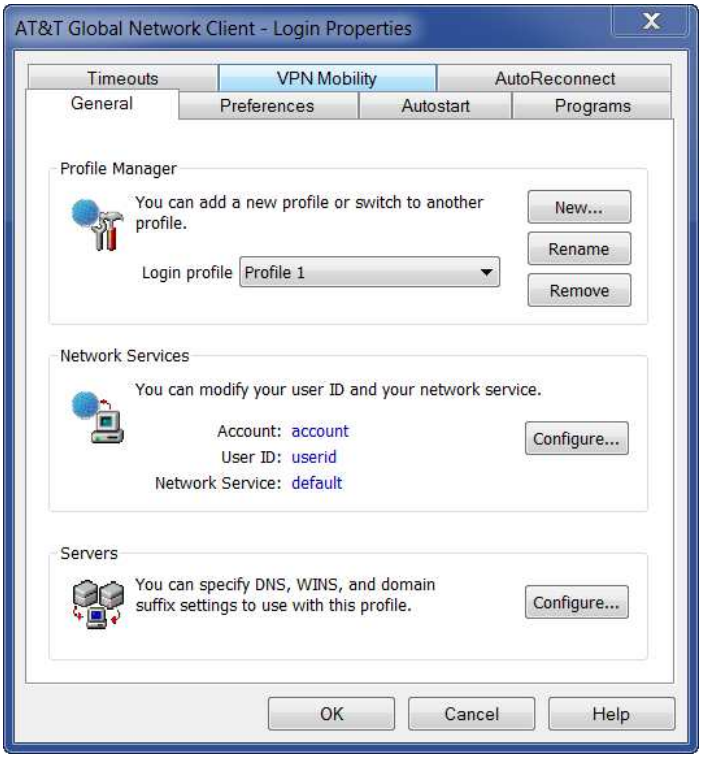


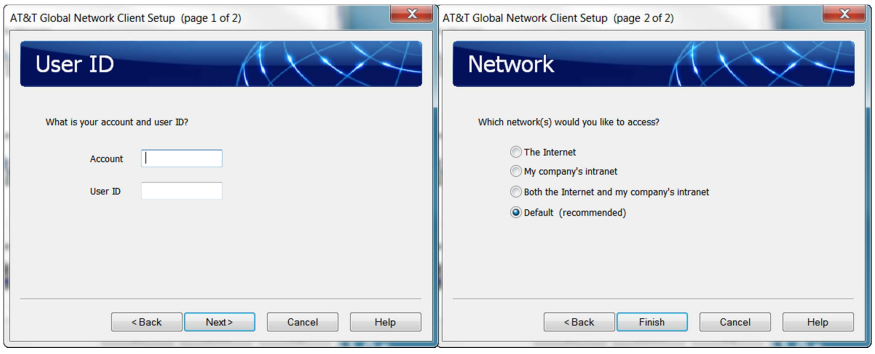
Figure 12: Login Properties Window

Profile Manager

Use the drop down box to activate an existing profile. Click **New…** to create a new profile. Click **Rename** to rename a profile. Click **Remove** to delete a profile.

Network Services

Click **Configure…** to change the Account, User ID, or Network Service. Your default network service is the service defined in the AT&T administration server for your specified Account and User ID. If you override the network service in the AT&T Global Network Client, you must be authorized for the new service in the AT&T administration server for a successful connection.



© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Figure 13: Configure Network Services Screens

Servers

DNS, **WINS**, and **Domain Suffix** configuration information is normally stored in the AT&T administration server. The AT&T Global Network Client automatically retrieves the values and updates the device to use the supplied values throughout the connection. Click **Configure…** to to verify or define your server information.

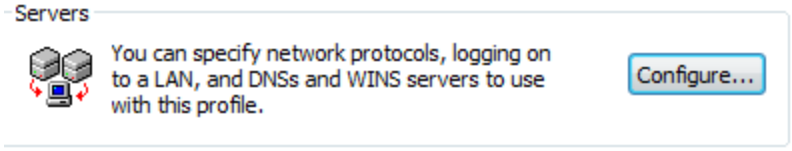

Servers
You can specify network protocols, logging on to a LAN, and DNSs and WINS servers to use with this profile.
Configure...

Figure 14: Servers Configure Button

To override the values defined in the AT&T administration server select **Use the following manual settings** and enter the corresponding values.

For **WINS** and **Domain Suffix** you also have the ability to select **Do not update** and the AT&T Global Network Client will not alter the specified settings when connected**.**

If you are required to be authenticated by a Windows Domain to logon to your Windows workstation, you can enable **Windows Logon**. Select **Yes, automatically start this program during Windows logon** to establish a network connection using the AT&T Global Network Client prior to your Windows logon. If you do not require a Windows Domain authentication to logon to your workstation, select **No, do not automatically start this program.**

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T Global Network Client Setup (page 4 of 4)
Windows Logon
Windows can automatically start this program at the Windows logon window.
Yes, automatically start this program during Windows logon.
No, do not automatically start this program.
< Back
Finish
Cancel
Help

Figure 15: Server Configure - Windows Logon Window

Preferences

Preferences define the settings for your connection. Preferences are organized by AT&T Global Network Client Profile. For more information about profiles see Profile Management in this guide.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

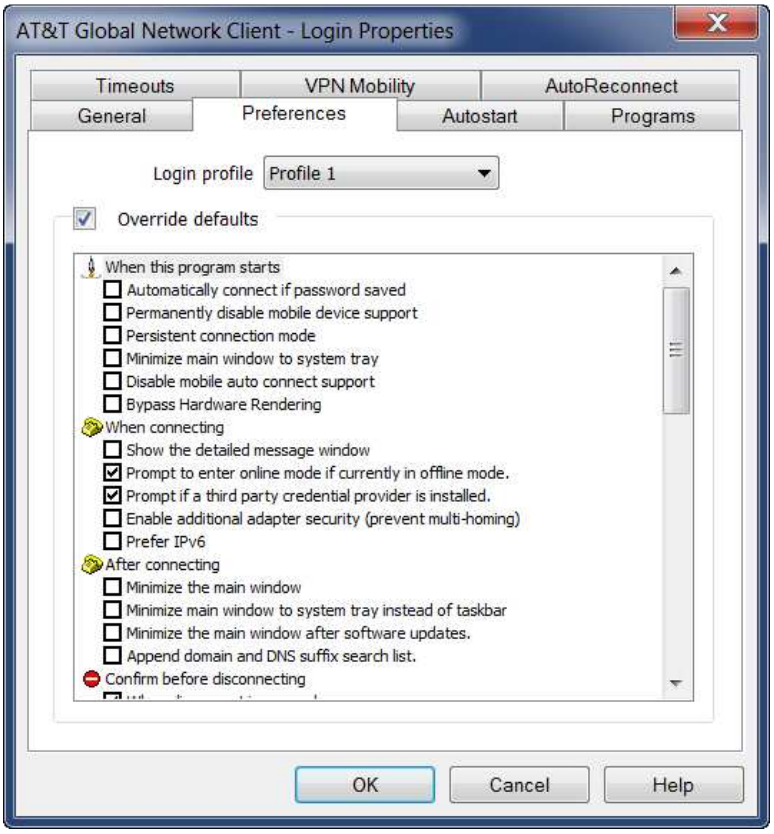


Figure 16: Login Properties - Preferences Window

Autostart

Autostart allows you to define programs to automatically launch at any of the following times:

- Before Connecting
- After Connecting
- After Performing Network Updates
- Before Disconnecting
- After Disconnecting

Autostart settings are organized by AT&T Global Network Client Profile. For more information about profiles see Profile Management earlier in this chapter of this guide.

Click the checkbox next to **Override defaults** to change any of the settings.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Click the **Add…**, **Change…**, and **Remove** buttons to configure the program information. Click on the arrow buttons to move a program up and down in the launch order.

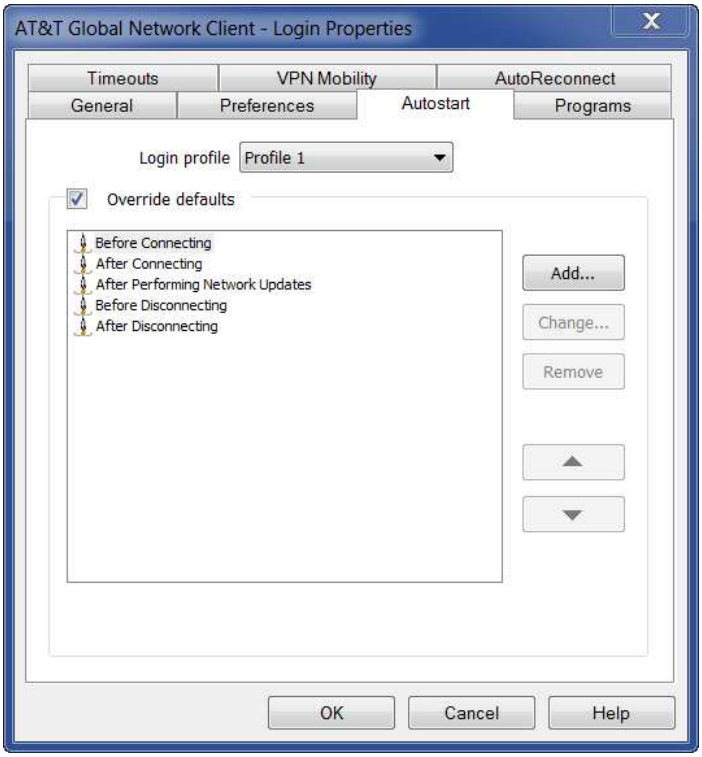


Figure 17: Login Properties - Autostart Window

Post Connection Script

In addition to starting the programs configured in the Autostart Preferences, the AT&T Global Network Client has been designed to automatically run a custom VBScript after connecting if provided by the Customer Account Administrator. The application will run a VBScript file named *PostConnectScript.vbs* if it is present in the directory in which the AT&T Global Network Client is installed. The system administrator may have to give execute permissions to this file. By having a script file (PostConnectScript.vbs), you have the flexibility to do a variety of common post connection tasks such as:

- Drive Mapping
- Launch your own VPN Client
- Launch messages to the User
- Record AT&T Global Network Client usage data

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

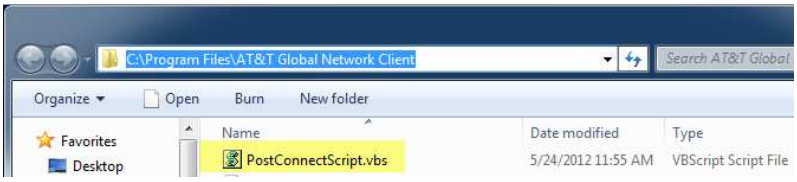


Figure 18: VBScript File Location and Name

Programs

The **Programs** tab allows you to specify which programs will be configured when connected to the network. Temporary updates are useful to eliminate or reduce the manual configuration needed before using the programs. The update values can be defined in the AT&T administration server by the Customer Account Administrator. No values are defined by default.

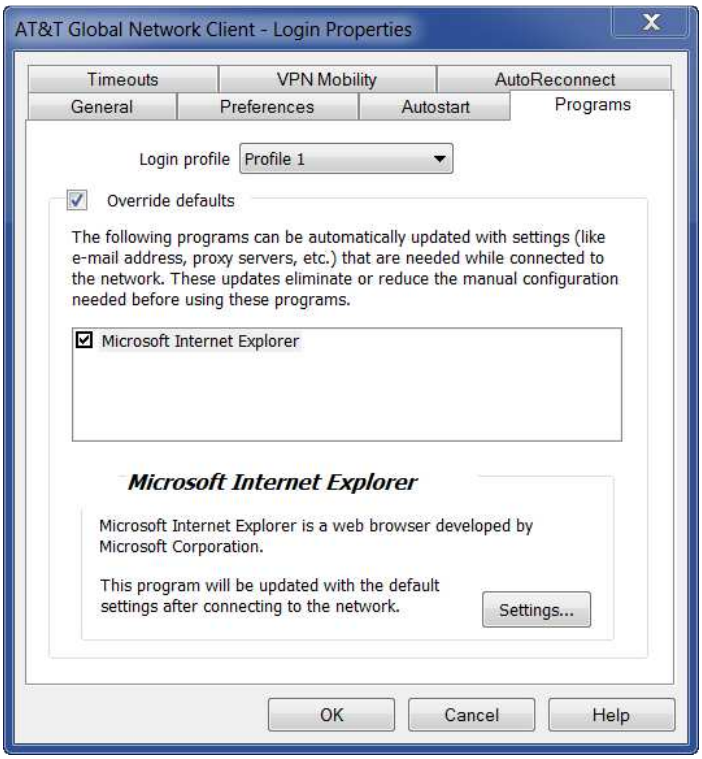

AT&T Global Network Client - Login Properties
Timeouts
VPN Mobility
AutoReconnect
General
Preferences
Autostart
Programs
Login profile
Profile 1
Override defaults
The following programs can be automatically updated with settings (like e-mail address, proxy servers, etc.) that are needed while connected to the network. These updates eliminate or reduce the manual configuration needed before using these programs.
Microsoft Internet Explorer
Microsoft Internet Explorer
Microsoft Internet Explorer is a web browser developed by Microsoft Corporation.
This program will be updated with the default settings after connecting to the network.
Settings...
OK
Cancel
Help

Figure 19: Login Properties - Programs Window

To prevent the use of the values from the AT&T administration server or to define new values, click **Override defaults** and select the program you wish to change. Click **Settings** to review the values and make any changes.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

For example, using the Programs tab, you can remove Microsoft Internet Explorer proxy settings while connected by clicking **Override Defaults**, selecting **Microsoft Internet Explorer**, clicking **Settings**, clicking to highlight **Auto-Proxy URL**, clicking **Manually update to**, and leaving the **Auto Proxy URL to use** field blank.

Timeouts

The AT&T Global Network Client supports two variations of **Timeouts** which can be configured by clicking **Override defaults**.

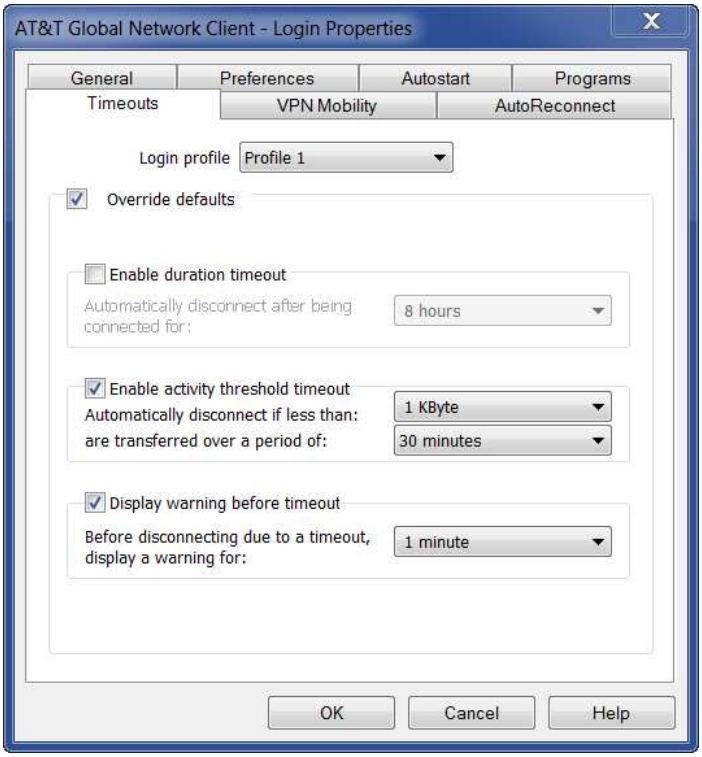


Figure 20: Login Properties - Timeouts Window

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Connection Features

The AT&T Global Network Client accommodates common transitions in network connectivity when users roam between networks or locations.

Persistent Connections

When enabled, the Persistent Connections feature will automatically connect or reconnect the AT&T Global Network Client with little or no user interaction. Persistent Connections can be used with all AT&T services as well as credential-less connections. For AT&T services, it must be configured both in the AT&T Global Network Client and the AT&T administration server. For Credential-less internet connections, the setting can be controlled with just the AT&T Global Network Client.

One example of the Persistent Connection advantage is a user with an active AT&T Global Network Client connection whose machine enters hibernation state, automatically disconnecting the AT&T Global Network Client connection. When the user returns and resumes their work, the AT&T Global Network Client enabled with Persistent Connections is designed to automatically initiate a connection attempt to establish connectivity, without action from the user. If the **Save Password** option is enabled, no user interaction is required to establish the new connection.

Persistent Connections does not maintain the current connection; when enabled, a new connection is established when necessary.

Configuration for AT&T Services (AT&T VPN or Business Internet Services)

The Persistent Connections feature requires:

- The **Persistent Connection** option must be enabled in the AT&T administration server. See Appendix A Central Configuration for additional information.
- The "Persistent connection mode" must be checked in the Login Properties of the AT&T Global Network Client.

User Preference

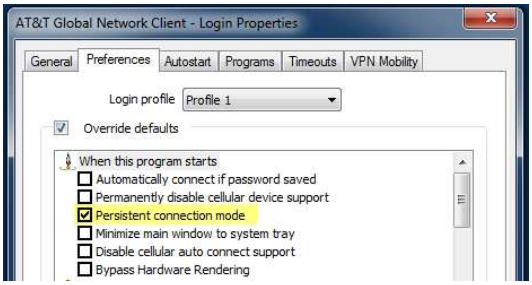
The user can be given the option to disable the use of Persistent Connections for one or more profiles using the **Allow Persistent Connections** property on the **Preferences** tab of the **Login Properties** dialog.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Persistent Connection Mode

When the **Persistent connection mode** property in the Login Properties dialog is disabled, a Persistent Connection will not be supported regardless of the value of the Persistent Connection Mode option in AT&T administration server.



The **Persistent connection mode** uses broadband, Wi-Fi or Mobile connections.

Enabling Persistent Connections during Installation

To simplify the end user experience for setting up and using Persistent Connections, a user can select the Custom setup type during installation and enable the default settings for the Persistent Connection mode. On the Installation Options dialog, under the Network Access Options, enable the checkbox next to Default settings for Persistent Connection mode.

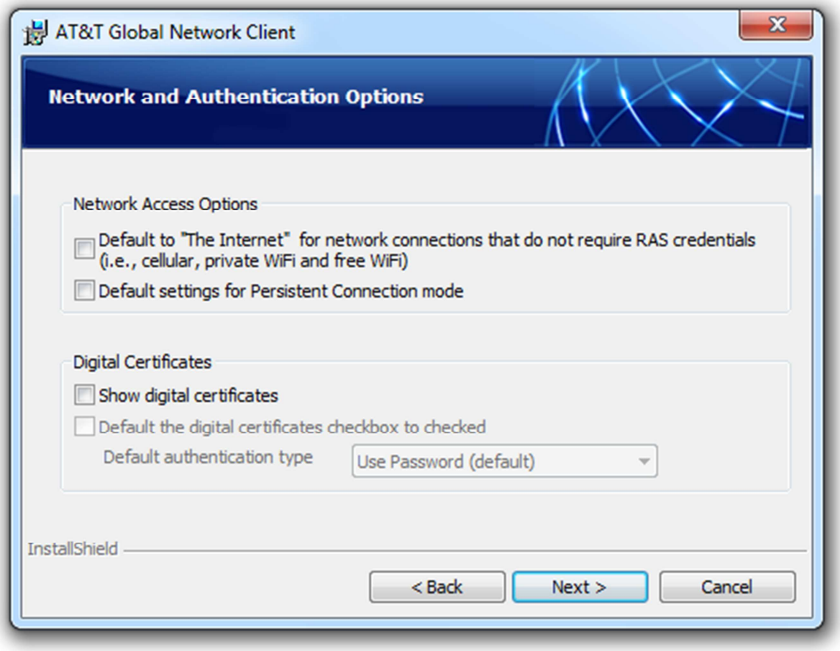

AT&T Global Network Client
Network and Authentication Options
Network Access Options
Default to "The Internet" for network connections that do not require RAS credentials (i.e., cellular, private WiFi and free WiFi)
Default settings for Persistent Connection mode
Digital Certificates
Show digital certificates
Default the digital certificates checkbox to checked
Default authentication type
Use Password (default)
InstallShield
< Back
Next >
Cancel

Figure 21: Installation Options – Default Settings for Persistent Connection mode

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

When this checkbox is checked, the installation program will:

- Create a shortcut to the AT&T Global Network Client executable in the All Users Startup folder.
- Enable the **Minimize main window to system tray** checkbox in the **When this program starts** section of the **Preferences** tab of **Login Properties**.
- Enable the **Minimize main window to system tray instead of taskbar** checkbox in the **After connecting** section of the **Preferences** tab of **Login Properties**.

Default Persistent Connection preferences can also be enabled by the Customer Account Administrator through customization. See the chapter on Customizations for more information on public properties of the AT&T Global Network Client.

VPN Mobility

When enabled, VPN Mobility attempts to maintain your VPN connection regardless of transitions in underlying network connectivity. VPN Mobility will not renegotiate a new VPN tunnel, but rather attempt to maintain an existing tunnel.

One example of the VPN Mobility advantage is a user with an active AT&T Global Network Client connection who is using a wired Ethernet network. The user unplugs his or her Ethernet cable to connect to the nearest Wi-Fi Hotspot Directory. The VPN tunnel will remain available in a suspended state on the VPN Server for a specified duration. VPN Mobility will automatically attempt to move the tunnel to the new network once the user associates to the Wi-Fi hotspot, without additional interaction from the user. Most applications will be unaware of the transition of the tunnel[4].

Unlike Persistent Connections, VPN Mobility attempts to maintain the same VPN connection, if it is unsuccessful, Persistent Connections must also be enabled for a new VPN connection to be established.

VPN Mobility does not require the Save Password option to be enabled.

Limitations

This feature is supported using AT&T propriety design; therefore the following limitations are required:

[4] Technology and applications dependent on TCP timeouts will not support the transition of the tunnel if the TCP timeout has expired before the tunnel was reestablished.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

VPN Mobility can only be supported using an AT&T SIG VPN Server as the tunnel terminating device for AT&T VPN Tunneling Services or the AT&T VIG with the AT&T Network-Based IP VPN Remote Access service.

VPN Mobility can only be supported using single-sign-on as the authentication method.

VPN Mobility will not work if the device enters the low power/hibernation state. If the user's device enters a low power or hibernation state the connection is automatically terminated.

Configuration

The VPN Mobility feature requires:

- The **VPN Mobility** option must be enabled in the AT&T administration server. See Appendix A Central Configuration for additional information.
- The **VPN Mobility Duration** option must be set to a value greater than zero in the AT&T administration server. See Appendix A Central Configuration for additional information.

Advanced Configuration

By default the VPN Mobility feature will sustain the VPN Connection using the default route. If multiple paths are available the prioritization is Ethernet, Wi-Fi, Mobile, Dial.

Users and administrators can define a custom network interface prioritization using the Login Properties dialog. Select **Login Properties**, **VPN Mobility** tab, enable the checkbox next to **Override defaults**, enable the checkbox next to **Operate in VPN Mobility mode**, select **Create my own network interface prioritization** and click **Configure**.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

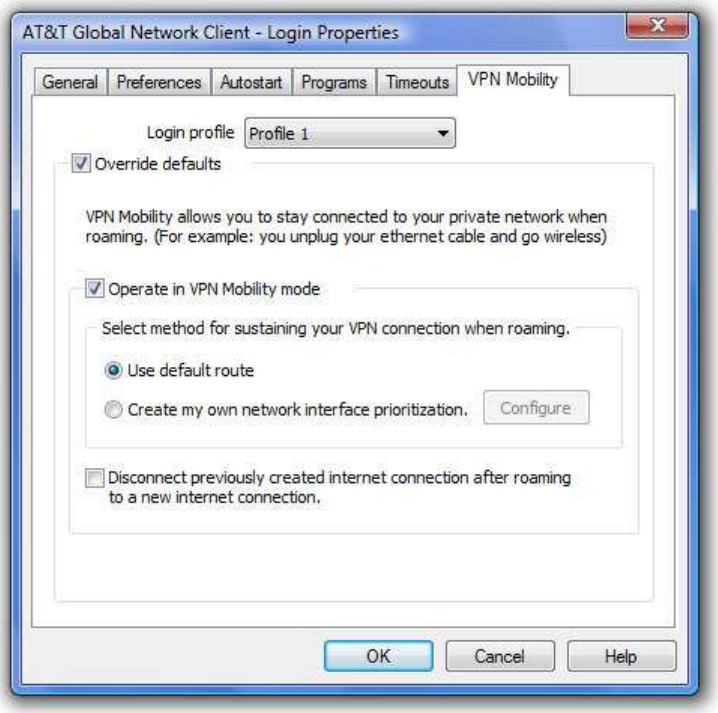

AT&T Global Network Client - Login Properties
General
Preferences
Autostart
Programs
Timeouts
VPN Mobility
Login profile
Profile 1
Override defaults
VPN Mobility allows you to stay connected to your private network when roaming. (For example: you unplug your ethernet cable and go wireless)
Operate in VPN Mobility mode
Select method for sustaining your VPN connection when roaming.
Use default route
Create my own network interface prioritization.
Configure
Disconnect previously created internet connection after roaming to a new internet connection.
OK
Cancel
Help

Figure 22: Login Properties/VPN Mobility

The **VPN Mobility Network Interface Prioritization** dialog allows the definition of the preference. Click **OK** to save.

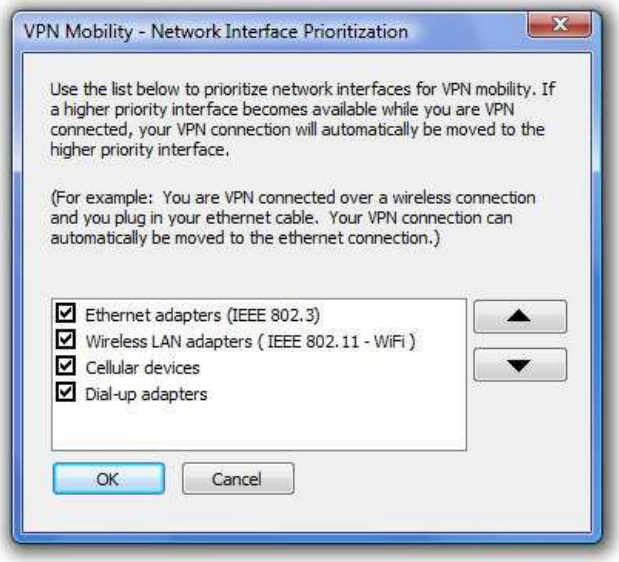

VPN Mobility - Network Interface Prioritization
Use the list below to prioritize network interfaces for VPN mobility. If a higher priority interface becomes available while you are VPN connected, your VPN connection will automatically be moved to the higher priority interface.
(For example: You are VPN connected over a wireless connection and you plug in your ethernet cable. Your VPN connection can automatically be moved to the ethernet connection.)
Ethernet adapters (IEEE 802.3)
Wireless LAN adapters (IEEE 802.11 - WiFi)
Cellular devices
Dial-up adapters
OK
Cancel

Figure 23: VPN Mobility Interface Prioritization

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

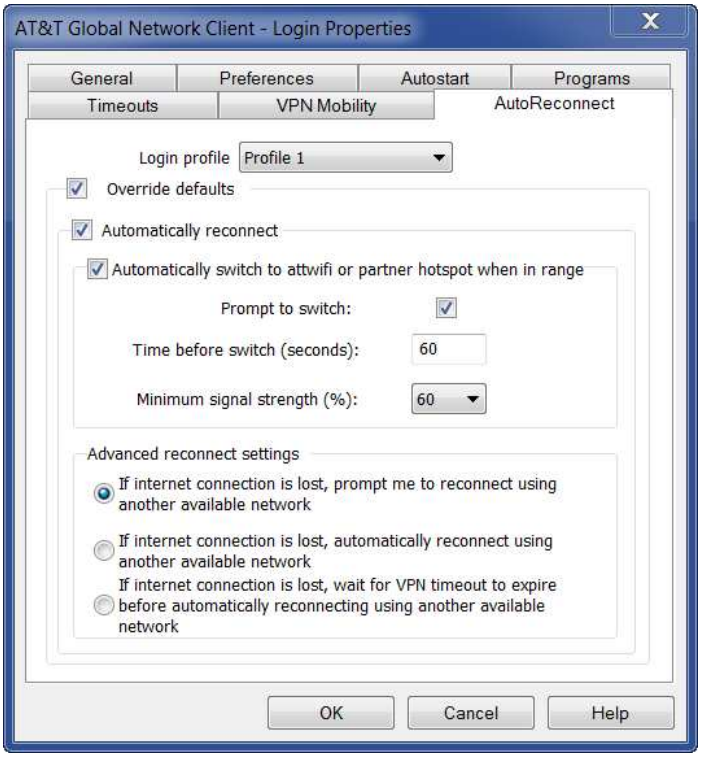
It is important to note that when a custom network prioritization is defined, the VPN connection will automatically be moved to the highest priority network interface even if the current network interface is still available.

User Preference

The user can be given the option to disable the use of VPN Mobility for one or more profiles using the **Operate in VPN Mobility mode** property on the **VPN Mobility** tab of the **Login Properties** dialog.

AutoReconnect

The AT&T Global Network Client supports connecting and reconnecting sessions for connection drops or for switching to AT&T Wi-Fi or AT&T Partner Hotspots when connected with a Mobile connection. These settings can be specified by your Customer Account Administrator in the AT&T Service Manager.



By setting the **Automatically reconnect** option, the existing connection will be re-established with another available connection. VPN sessions can also be re-established without having to re-enter credentials.

The **Automatically Switch to attwifi...** option will switch your connection over to one of AT&T's free Wi-Fi hotpots or partner hotspot when connected with a Mobility connection. The target hotspot must have a "strong" signal of at least 60% before the client will switch to Wi-Fi. The **Time before switch** option is a

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

safeguard against switching to AT&T's Wi-Fi in a drive-by/drive away siutation and losing your existing session altogether. The switch can be automatic or prompted depening on the **Prompt to switch** setting.

Advanced reconnect settings allow you to control how the Autoreconnect will happen: Automatically, Prompt or after the VPN session times out.

Prevent Multi-Homing

When enabled, the Prevent Multi-Homing feature prevents the ability for other network interfaces to be made available once a connection has been established through the AT&T Global Network Client. For example, this feature prevents an Ethernet or Wi-Fi connection from becoming active while connected over a mobile connection.

Additionally, the user will not be able to install or enable any new network interfaces through the Windows Control Panel while connected.

Prevent Multi-Homing Feature insures all traffic flows through the active connection established by the AT&T Client: Use it if you have multiple connections and need additional adapter security.

Configuration

The Prevent Multi-Homing feature can be enabled by the user unless the option to do so is disabled by the Customer Account Administrator through customization. See the chapter on Customizations for more information on public properties of the AT&T Global Network Client.

User Preference

The user can be given the option to enable the Prevent Multi-Homing feature for one or more profiles using the **Enable additional adapter security (prevent multi-homing)** property on the **Preferences** tab of the **Login Properties** dialog.

AutoConnect Feature

Certain Mobile devices allow the AT&T Global Network Client to monitor the Connected state. When supported by the mobile device, if the AT&T Global Network Client recognizes a mobile connection is active, and the default Profile is Internet, the AT&T Global Network Client will reflect the Connected state when the AT&T Global Network Client is launched.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Software Updates

The AT&T Global Network Client is designed to automatically attempt to update the following components after initial installation and on regular intervals thereafter:

- Hotspot Directory (Wi-Fi locations, phone numbers, etc.)
- AT&T Global Network Client software
- Mobile firmware, Mobile SDK, Mobile Drivers
- Lightweight Policy Enforcement files
- Dynamic customizations files

Depending on your Operating System, Microsoft Windows Administrator Rights may be required for automatic software update of the AT&T Global Network Client software.

Suppress Program Updates

Because many customers want to control deployment of software to their corporate devices, the Customer Account Administrator can opt to suppress the check for Program Updates. This capability can be suppressed using a Windows Installer public property. See the Public Properties section later in this guide for additional details.

User Permissions

Administrator rights are required to update the AT&T Global Network Client software. Hotspot Directory updates, mobile firmware updates and dynamic customization updates can be applied without Administrator rights.

Software Update Process

Updates for the AT&T Global Network Client software are downloaded from ftp://165.87.194.246. Updates to the Hotspot Directory are downloaded from http://32.97.166.118. The update service attempts to download the current version file from the server directly, without using any proxy settings. If the attempt fails, the update service will attempt to retrieve the version file using the proxy settings stored in Microsoft Windows Internet Options. If the file was successfully retrieved using the attempt through the proxy server, future attempts will automatically be retrieved using the proxy.

The available versions are compared against the installed versions of the AT&T Global Network Client software and the Hotspot Directory to determine if a newer version is available.

Automated Check for Updates

A service that periodically checks for updates to all AT&T Global Network Client software components is installed with the AT&T Global Network Client and runs in the background when your Windows machine boots up. It does not require the AT&T Global Network Client to be running.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

If an update is available, the download is initiated. Downloads in the background run at low priority and only occur when the workstation is idle. A system tray icon will be displayed when checking or retrieving and installing updates. If the user holds the mouse pointer over the icon, the current status of the operation will be shown. If the user double-clicks the icon, the Software Updates application will be run, showing the detailed status of the update and allowing the end user to cancel the update if they wish.

The software update service will check for new updates for all software components every 14 days. The interval between updates can be customized by the Customer Account Administrator.

If the Hotspot Directory, Lightweight Policy Enforcement files, or Dynamic customizations files are newer than the installed files, the updates will be automatically downloaded and installed without prompting the user.

If a Software Update is available, the updated installation package will be downloaded. The next time the user launches the AT&T Global Network Client, the user will be prompted to install the newer version of the AT&T Global Network Client. If mobile firmware needs to be updated, the user is also prompted.

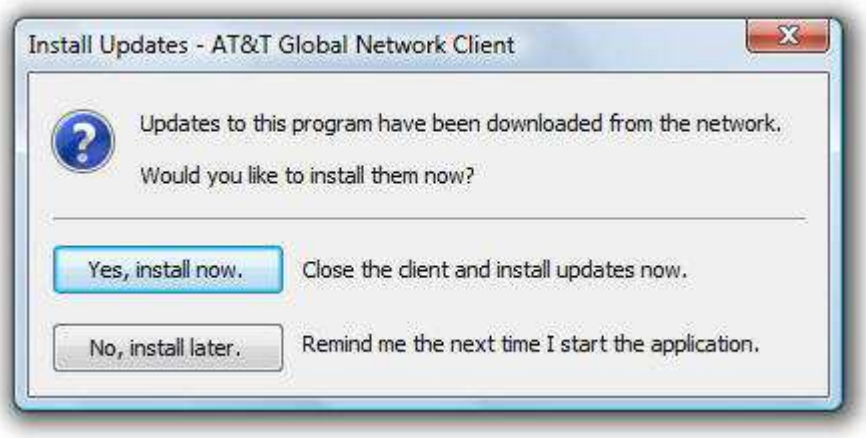

Install Updates - AT&T Global Network Client
Updates to this program have been downloaded from the network.
Would you like to install them now?
Yes, install now.
Close the client and install updates now.
No, install later.
Remind me the next time I start the application.

Figure 24: Install Updates

Manual Check for Updates

To manually initiate a check for updates, click **Check for Updates** from the **Help** panel on the left hand side of the main window.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

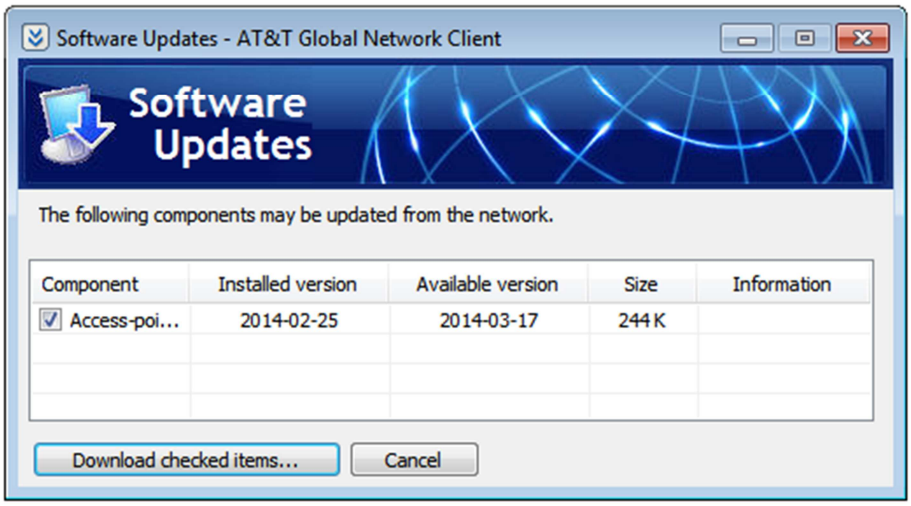


Figure 25: Software Updates Window

The **Software Updates** window will list the components and the version information. If an update is available, the component will be checked. Click **Download checked items…** to complete the update process. All checked components will be updated.

Feature Specific Updates

Some of the features of the AT&T Global Network Client can be updated independently of the AT&T Global Network Client. Those features are:

- Lightweight Policy Enforcement
- Mobile SDK
- AT&T Mobile Drivers
- AT&T Mobile Device Firmware

Installation packages which update each of these features independent of the complete AT&T Global Network Client installation package are made available with each new version of the AT&T Global Network Client. Significant programming interface changes may necessitate an update in order to take advantage of the latest features of the AT&T Global Network Client. The feature specific installation packages can be used to upgrade an existing installation of the AT&T Global Network Client to a newer version of the selected feature without upgrading the entire AT&T Global Network Client. As an administrator, you can deploy these updates using your preferred software distribution tool, or, you can request AT&T to host the update packages on a custom download location on an AT&T server. Having AT&T host the downloads will require Service Manager configuration or a customized installation package, both of which can be arranged with your AT&T account team.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Uninstall

Local Uninstall

The AT&T Global Network Client is removed via the **Windows Control Panel**, **Programs and Features** option.

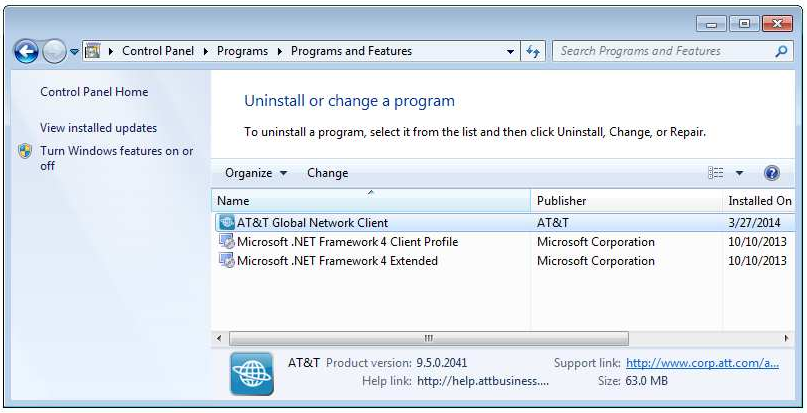


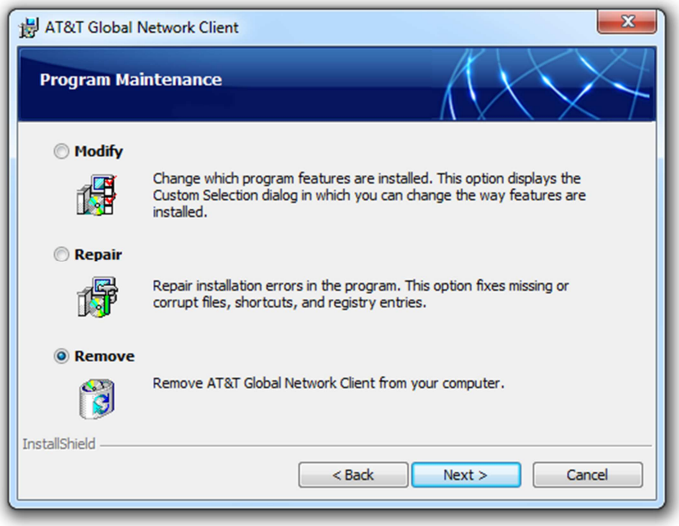
Figure 26: Programs and Features Window

Uninstall

The Programs and Features Uninstall option is not supported for the AT&T Global Network Client; to uninstall click Change and follow the directions below.

Change

Click **Change** on the **Programs and Features** window list to **Modify**, **Repair** or **Remove** the AT&T Global Network Client program


AT&T Global Network Client
Program Maintenance
Modify
Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.
Repair
Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.
Remove
Remove AT&T Global Network Client from your computer.
InstallShield
< Back
Next >
Cancel

Click **Remove** and click **Next>** to continue.

Figure 27: Modify, Repair, Remove Welcome

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Program files will be removed. You can also select which user settings are removed. Select **Leave all user settings on the computer. (default)** to leave user information such as account and user ID as well as profile information on the computer. Select **Remove only my user settings** to remove only the settings stored for the current user. Select **Remove settings for all users on this computer** to remove all AT&T Global Network Client user settings on the computer. Click **Next>** to continue.

AT&T Global Network Client
AT&T Global Network Client
The installation will allow you to modify, repair, or remove AT&T Global Network Client. To continue, click Next.
Product Version: 9.5.0.2057
< Back
Next >
Cancel

Figure 28: Program Maintenance Window

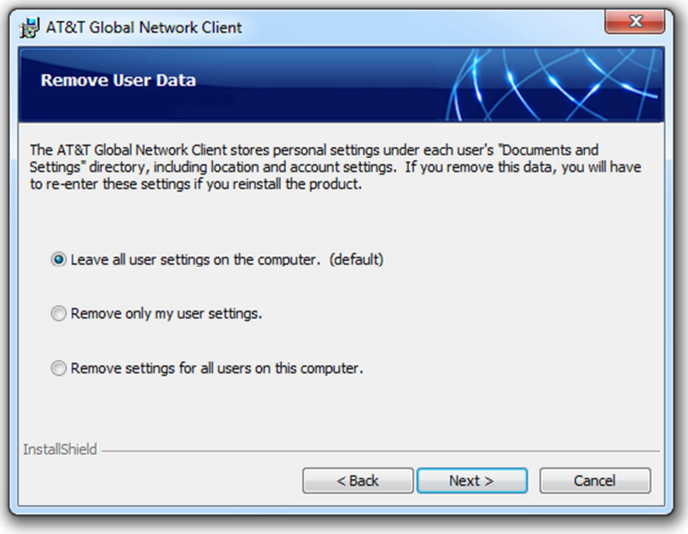
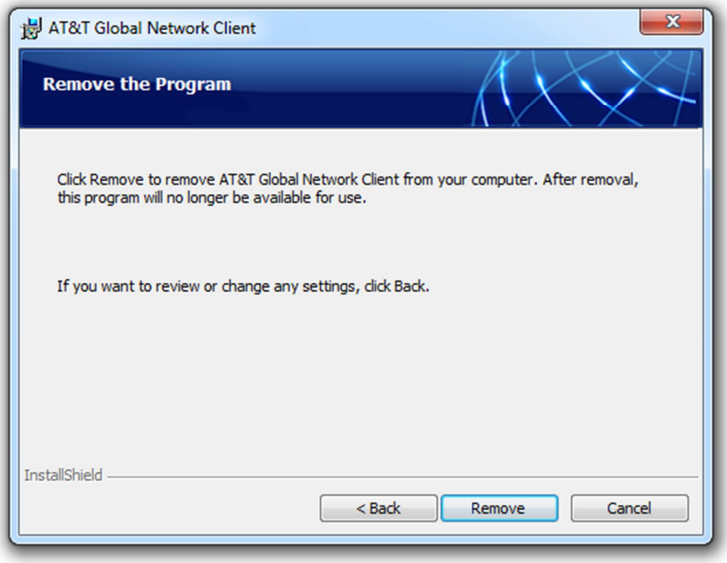

AT&T Global Network Client
Remove User Data
The AT&T Global Network Client stores personal settings under each user's "Documents and Settings" directory, including location and account settings. If you remove this data, you will have to re-enter these settings if you reinstall the product.
Leave all user settings on the computer. (default)
Remove only my user settings.
Remove settings for all users on this computer.
InstallShield
< Back
Next >
Cancel

Figure 29: Remove User Data Window

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Click **Remove** to continue.


AT&T Global Network Client
Remove the Program
Click Remove to remove AT&T Global Network Client from your computer. After removal, this program will no longer be available for use.
If you want to review or change any settings, click Back.
InstallShield
< Back
Remove
Cancel

Click **Finish**.

AT&T Global Network Client
Removal Completed
The installation has successfully uninstalled AT&T Global Network Client. Click Finish to exit the wizard.
< Back
Finish
Cancel

Reboot May Be Required:
You will be prompted if you must reboot your workstation after removing the AT&T Client.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Remove Warning

The AT&T Global Network Client cannot be removed while it is running. If you attempt to remove the AT&T Global Network Client when it is running you will receive an error.

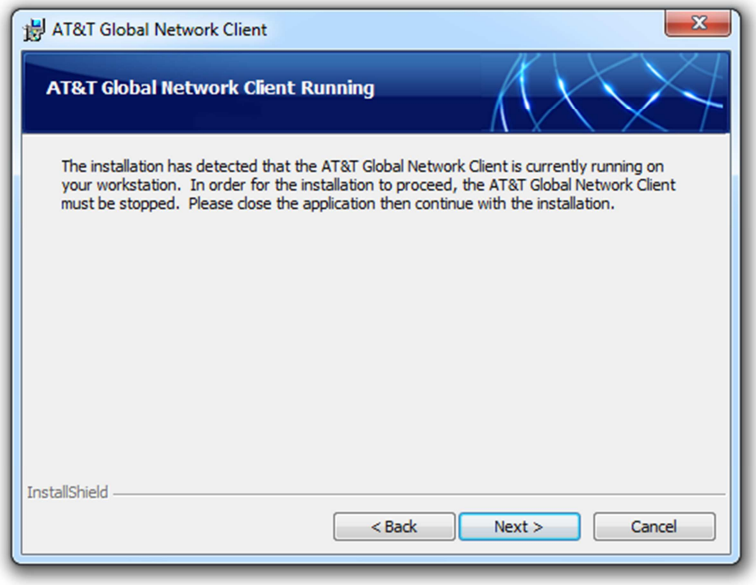

AT&T Global Network Client
AT&T Global Network Client Running
The installation has detected that the AT&T Global Network Client is currently running on your workstation. In order for the installation to proceed, the AT&T Global Network Client must be stopped. Please close the application then continue with the installation.
InstallShield
< Back
Next >
Cancel

Figure 32: Client Running, Remove Warning Window

Remote Uninstall

If you used a desktop software management server to distribute the AT&T Global Network Client, you may be able to use the server to remove the package. You must initiate a reboot or have users manually restart or shutdown after the AT&T Global Network Client is removed to confirm the software is fully uninstalled.

Command Line Uninstall

Advanced users can uninstall using the command line. When using the command line, Windows Installer public properties can be used to control the type of uninstall performed. More information can be found in the Public Properties table on page 50; reference the REMOVE_USER_SETTINGS property.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Customizations

The AT&T Global Network Client can be customized by you, the Customer Account Administrators to streamline setup and define specific features for your users.

Advanced Customizations Using Windows Installer

The AT&T Global Network Client installation is packaged using Microsoft Windows Installer and InstallShield® 2013. The installation of the AT&T Global Network Client can be customized. A number of Windows Installer public properties are available to specify details of the installation. Additionally, Windows Installer provides native capabilities that can be used to specify features to be installed and to control the installation experience.

AT&T Global Network Client Features

The AT&T Global Network Client contains a number of Windows Installer Features. Each Feature defines a required or optional component of the AT&T Global Network Client. The AT&T Global Network Client Ffeatures are described below.

Feature	Description
Net_Client	Installs the AT&T Global Network Client that is used for all AT&T Services. This feature is required.
Firewall_GUI	Allows a user to turn the AT&T Global Network Client Firewall on and off while the AT&T Global Network Client is not running.
VPN_Client	Installs VPN software for connecting to your company's private network. **NOTE**: Not available in the installation package used for export
APD-NA	Hotspot Directory Database for North America
APD-EMEA	Hotspot Directory Database for Europe, Middle East and Africa
APD-SA	Hotspot Directory Database for South America

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

APD-AP	Hotspot Directory Database for Asia Pacific
APD-PRC	Hotspot Directory Database for People's Republic of China
APD-DIAL	Directory Database for Global Dial Locations
PLAP	Provides the ability to connect to the network before logging onto Windows 7 and Windows 8. This feature can be seen by selecting Custom Installation Path in any Edition.
LPE	Installs the Lightweight Policy Enforcement Feature and provides for the visibility of the Security Status portion of the AT&T Global Network Client Main Window.
Languages	Installs English, French, German, Japanese, and Spanish language support. Each language is a sub-feature under the Languages feature. English is required, other languages are optional.
T6_Client	Installs device drivers for the T6 Client. This provides support for IPv6.
CellularDrivers, ATTBeamDrivers	Installs the Mobile Device Drivers. This feature is an optional feature. Drivers are available for Netgear/Sierra Wireless devices.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Public Properties

The installation packages contain a number of public properties that can be set on the command line or within a transform. The properties in the table below govern some behaviors of the setup.

Important Note: Some public properties ***should not*** be used along with the CONFIG_FILE public property. Some public properties (noted with "Use XML") will generate a config.xml which will be overwritten by the CONFIG_FILE. If using CONFIG_FILE, please include all customizations in the config.xml only.

Property	Use XML	Intended Use & Value Information
ACCOUNT	X	This property can be set to pre-configure the account used to connect to the network
AUTOCONNECT_CONTROL_ALLOWED	X	Set this property to "yes" to show the Automatic Mobile Connection option on the Mobile Menu. Default: "yes"
CELLULAR_ROAMING_ALLOWED		Set this property to "yes" to allow the AT&T Global Network Client to connect while the mobile device is roaming, OR "no" to prevent the AT&T Global Network Client from connecting while the mobile device is roaming, OR "prompt" to prompt the user before connecting while the mobile device is roaming. Default: "prompt"
CERT_SHOW	X	Set this property to "Y" to set the AT&T Global Network Client to show the "Login using a Digital Certificate or Smart Card" checkbox on the User ID panel of the Setup Wizard. Default: blank (not set)
CERT_SHOW_SET	X	Set this property to "Y" to select the "Login Using a Digital Certificate or Smart Card" checkbox for all new user profiles. Default: blank (not set)
CERT_DEFAULT_USE		Set this property to "1" to make the AT&T Global Network Client look for certificates only on the Smart Card. Default: blank (not set)

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Property	Use XML	Intended Use & Value Information
CONFIG_FILE		This property can be set to the name of an xml file which contains the settings for a Trusted LAN configuration or Client Profiles configuration. If a full path is not specified, the installation package will look for a file in the same directory as the installation source. See page 62 for customizations in the CONFIG_FILE section for more information. Default: blank (not set)
CUSTOM_APN		Set this property if you are using a custom APN to connect with your Mobility device.
CUSTOM_APN_USERNAME		Set this property if you are using a custom APN and need a user name to connect with your Mobility device. * Only do so if directed by your AT&T Account Representative
CUSTOM_APN_PASSWORD		Set this property if you are using a custom APN and need a password to connect with your Mobility device. * Only do so if directed by your AT&T Account Representative
DEFAULT_AUTOCONNECT_MODE		Set this property to "ENABLE" to enable auto-connect on client start if the detected hardware supports the autoconnect feature. Set to "DISABLE" to disable the autoconnect feature when the AT&T Global Network Client starts. Default: "NOCHANGE"
DESKTOP_SHORTCUT		Set this property to "1" to install a desktop shortcut. Set it to an "" (empty string) (i.e. DESKTOP_SHORTCUT= "") to not install a desktop shortcut. Default: "1"
DISABLE_CELLULAR_SDK		Set this property to "1" to disable mobile SDK integration. Default: "0"

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Property	Use XML	Intended Use & Value Information
FIREWALL_STATE		Set this property to "on", "off" or "disabled" on the command line to control the initial state of the AT&T Global Network Client Firewall. Setting the state to "on" defaults the AT&T Global Network Client Firewall on causing it to discard unsolicited traffic. Setting the state to "off" causes the AT&T Global Network Client Firewall to allow all traffic. Setting the firewall to "disabled" makes it so the AT&T Global Network Client Firewall will not be used as a firewall.
HIDE_SAVE_PASSWORD	X	Set this property to "1" to hide the Save Password or Save Pin option on the Network Logon dialog. See Figure 10 for the checkbox option described. Default: "0"
INTERNET_ONLY	X	Set this value to "1" to allow the users to connect directly to mobile and Wi-Fi (private and free) Internet networks without entering AT&T Global Network credentials (Account, User ID, and Password). Default: "0"
LAUNCHPROGRAM		Set this value to "1" to pre-select the launch program checkbox on the setup complete dialog of the installation. Default: "1"
LOCK_TO_3G		Set this value to "1" set and lock a mobility device to 3G mode when using a 3G Custom APN. Set this value to "0" to set the mode to default service.
LPE_COMPLIANCE_THRESHOLD		Set this value to the number of failed compliance checks allowed before the AT&T Global Network Client performs the compliance failure action; with a default value of "0", the AT&T Global Network Client will immediately handle compliance failures.
LPE_FILE	X	Set this value to prevent connections if a specificied file does not exist on the system. Example: LPE_FILE=C:\Windows\compid.txt Note: The LPE *feature* does not need to be installed.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Property	Use XML	Intended Use & Value Information
LPE_OS_RANGE	X	Set this value to prevent connections on specific Operating Systems. Use the numeric version of an Operating System(s) you wish to block. Example: Windows Vista through Windows 7 RTM: LPE_OS_RANGE=6.0.6000-6.1.7600 Note: The LPE *feature* does not need to be installed.
LPE_REG	X	Set this value to prevent connections if a specificied registry hive does not exist in the HKEY_LOCAL_MACHINE branch. Example: LPE_REG="SOFTWARE\YourCompany\Asset" Note: The LPE *feature* does not need to be installed.
MINIMIZE_AFTER_CONNECTING		Set this property to "1" to minimize the main window to task bar after connecting. Default: "0"
MINIMIZE_TO_SYSTEM_TRAY		Set this property to "1" to minimize the main window to system tray after connecting. Default: "0"
MULTIHOMING_CLIENT_ADDITIONS		Specifies the VPN Clients to exclude when preventing multi-homing: Cisco Client: Cisco All Cisco Clients: CiscoAll Juniper Client: Juniper CheckPoint Client: Checkpoint Example: MULTIHOMING_CLIENT_ADDITIONS=Cisco
NS_FROM_VPN_SERVER		Use the name servers supplied by the VPN server instead of the values supplied from the Service Manager
PASSWORD	X	Used to specify the password for a pre-configured profile

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Property	Use XML	Intended Use & Value Information
PROFILENAME	X	Used to specify the profile name for a pre-configured profile
PROGRAM_GROUP		Set this property to full path to the start menu program group (i.e. C:\Documents and Settings\<Username/All Users>\Start Menu\Programs\Group Name) in order to specify an alternate Program Group for the installation. Default: <blank>
QUICKLAUNCH_ SHORTCUT		Set this property to "1" to install a program shortcut in the Quick Launch bar. By default no Quick Launch shortcut is created. If a shortcut is created in the Quick Launch bar, but the user's Quick Launch bar is not already shown, they will need to display their Quick Launch bar. The installation package will not alter the current state of a user's Quick Launch bar. Default: <blank>
REMOVE_USER_ SETTINGS		This property controls whether to remove user settings during uninstallation. Specifying "None" causes the setup to leave user settings on the computer. Specifying "Me" causes the setup to delete the entire [LocalAppDataFolder]AGNS directory. Specifying "All" causes the setup to remove the entire [LocalAppDataFolder]AGNS for every user account on the computer. Default: "None"
SHARED_SETTINGS		Set this to "1" for the AT&T Global Network Client to use the Common Application Data folder on the workstation, instead of the users application data folder for settings and profiles. This enables all users on a workstation to share the same settings and profiles. This value is automatically set to "1" for new installations that include the GINA feature. Default: "0" ("1" for new PLAP installations)

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Property	Use XML	Intended Use & Value Information
SHOW_DIAL		Set this to "1" for the AT&T Global Network Client to show the Dial Connection. By default, the Dial method of connecting is not shown. Default: "0"
SKIPWINLOGONCHECK		Set this property to "1" to bypass the check for the install running on the WinLogon desktop. Default: <blank>
SUPPRESS_UPGRADE_REBOOT		Set this property to "1" to suppress the upgrade reboot when installing a new version of the AT&T Global Network Client to a system which already has a previous version installed. Set to "0" to allow a reboot during upgrade. Default: "0"
SUPPRESS_PROGRAM_UPDATES		Set this property to "1" to suppress the check for program updates. Other updates, such as Hotspot Directory database updates, will still occur. This property is not set by default.
TRUSTED_DOMAINS		Set this property to a comma delimited list of Connection-specific DNS Suffixes for which the firewall should be disabled for the Trusted Domain Configuration
UPDATE_OVER_METERED		Used to control whether or not the updates are downloaded over metered/low-bandwidth connections (mobile and dial). The possible value are "yes", "no", and "prompt". The default value is "prompt".
USERID	X	This property can be set to pre-configure the User ID used to connect to the network.
VNIC_CON_NAME		This is the name of the network connection that will be show in the Windows Network Connections window. *Ideally this value SHOULD NOT be changed*. Default: "AT&T Global Network Virtual Network Adapter"

Shortcuts

Name	Location	Target File

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T Global Network Client	Desktop	NetClient.exe
AT&T Global Network Client	[ProgramMenuFolder]AT&T Global Network Client	NetClient.exe
Customer Support	[ProgramMenuFolder]AT&T Global Network Client	NetHelp.exe
Firewall Settings	[ProgramMenuFolder]AT&T Global Network Client	NetFW.exe

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Common Windows Installer Properties

Network administrators frequently deploy applications via a command line or with a transform. Properties can be set in a transform and on the command line, as well.

Property	Example	Intended Use
ADDLOCAL	ADDLOCAL=PLAP	List the features you want to install locally, separated by commas.
INSTALLDIR	INSTALLDIR=C:\Program Files\AT&T Global Network Client	The main installation directory for the product.
PRODUCTNAME	AT&T Global Network Client	The name of the application.

Using the Command Line to Customize Installation

Using the Public Properties and understanding the Features available in each AT&T Global Network Client Edition, you can customize your installation package using command line switches and parameters.

When using command line customization, any default parameters normally set by the AT&T Global Network Client installation are superceded by the parameters set on the command line. If using command line customization you must replicate the default parameters normally set by the AT&T Global Network Client program (such as generation of an installation log).

Windows Installer command line switches are described on the Microsoft MSDN site at: http://msdn2.microsoft.com/en-us/library/aa367988.aspx

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Example Command Line Customizations

Example	Command
Silent installation with a Desktop Shortcut	msiexec /i agnc.msi /qb
Silent installation with No Desktop Shortcut	msiexec /i agnc.msi DESKTOP_SHORTCUT="" /qb
Install only specific Mobile Drivers	msiexec /i agnc.msi ADDLOCAL=Net_Client,ATTBeamDrivers/qb!
Completely Silent Installation[5]	msiexec /i agnc.msi /qn
Installation with logging	msiexec /l agnc.msi /l*v install.txt
Executable installation with logging	agnc.exe /v"/l*v install.txt"
Interactive Hook Mode GINA installation	msiexec /i agnc.msi ADDLOCAL=ALL
Silent installation without AT&T Global Network Client Firewall	msiexec /i agnc.msi ADDLOCAL=Net_Client,VPN_Client,PLAP /qb
Silent Uninstallation Using the MSI Package	msiexec /x agnc.msi /qb
Suppress Reboots	msiexec /i agnc.msi REBOOT=ReallySuppress

Creating a Windows Installer Transform

A transform is available if you are unable to create the customization you desire using only command line options. A transform provides advanced customization which is applied to the standard installation package at the time of installation.

One important capability of a transform is that if done properly, it can be written to apply to several versions of the AT&T Global Network Client Installer packages. Also, patches that are created for the

[5] Beginning with Version 8.0, using the /qn option for a silent installation will remove the user interface from the AT&T Global Network Client installation and will persist and chain to any subsequent additional features or third party installations included with the AT&T Global Network Client installation package

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

standard AT&T Global Network Client Installer package should also apply to AT&T Global Network Client packages that have been customized with a transform if the transform has been implemented correctly.

To preserve as much as possible of the typical behavior of the standard Windows Installer package, your transform should make as few changes as possible. That means that you should first try to accomplish the modification by changing values in the Property table, rather than by making more extensive changes in the MSI database. It is recommended all changes are done with a minimalist approach to avoid unintended consequences.

Tools to Create a Transform

Microsoft Windows Platform SDK contains tools which can assist you in creating a transform. You must obtain and install the Windows Platform SDK relevant to your operating system to have access to the tools.

The Microsoft tool named Orca can open and edit MSI transform files. When Orca is installed as part of the Windows Platform SDK, you can right click on MSI files and select the option **Edit with Orca**.

When viewing an AT&T Global Network Client MSI file with Orca the public properties will be shown in the Orca Property Table. Properties not listed in the Orca Property Table, but listed in this document can be added to the Orca Property Table for editing. Select **Add Row** in the Orca Property Table to add fields and corresponding values.

Common Changes Customized via a Transform

Item	Notes
INSTALLDIR property	When specified during an upgrade, the installation package will honor an installation directory change for a Major Upgrade. Minor updates must install to the same directory as a previous installation.
PACKAGE_ID property	The default value is "default". This change also requires additional database files provided by AT&T via a customization that must be included with the package.
PACKAGE_VERSION	An optional revision number for packages which have used the same PACKAGE_ID. This change also requires additional database files provided by AT&T via a customization that must be

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Item	Notes
	included with the package.
ProductName property	
Start menu folder	
Names of shortcuts	
The selection states of features, such as GINA	
Whether various dialogs appear in the UI	
Captions on the dialogs	This change also requires additional database files provided by AT&T via a customization that must be included with the package.
The installation of additional files (i.e. Data\Custom)	These files should be "new" files that are not in the original setup.

Things That Must Be Avoided

Performing any of the following using a transform will make future patches and upgrades difficult or potentially impossible.

- Renaming the original MSI package.
- Using a transform to deploy updated files that the MSI package already deploys. (There is one exception for passwordrules.chm.)
- Removing any components.
- Changing the ProductCode, UpgradeCode, or Package Code.
- Changing the ProductVersion property.

Recommended Actions via a Transform

If you are going to perform any of the following, the recommended approach is to use a Windows Installer Transform.

Adding Files

Only add new files in a transform. Do not remove any key files from any existing components.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Updating Files

Use patches or upgrades to update files that exist in the original setup. Do not use a transform to cause the setup to install newer files than were in the original setup because that will make the transform invalid for future versions of the setup.

Customizing Your Password Rules

Password rules are contained in the file **"passwordrules.chm"**. The **"Never Overwrite"** property for the component that installs the file **"passwordrules.chm"** has been set to **"Yes"**. Therefore, it is possible to include a different version of this single file in a transform and replace the file that is deployed in the original MSI package. Since this file will never be overwritten, it will be preserved during upgrades and patches.

Changing the Installation Directory

Change the installation directory in the setup by modifying the value of **INSTALLDIR** in the Directory table. When specified during an upgrade, the installation package will honor an installation directory change for a Major Upgrade. Minor updates must install to the same directory as a previous installation.

Changing the Application Name

You can change the name of the application name by modifying the **ProductName** property in the **Property** table. You can modify the names of the shortcuts by changing the values in the **Name** field in the **Shortcut** table.

Making the Transform Apply To Future Versions

Transforms offer several validation checks that can occur before the installation begins. The validation can occur on the **UpgradeCode**, **ProductCode**, **ProductVersion**, and **ProductLanguage** properties. To make the transform apply to future versions of the product, you should eliminate the validation checks or check only the **ProductCode**.

The Project Settings dialog in InstallShield configures which validation checks occur at runtime. To open this dialog, click **Project** then **Settings** from the menu.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Customization Using a config.xml File

If you require more than a few simple customizations for your deployment which can all be accommodated using Windows Installer public properties, you can use a config.xml file to specify all of your customization and configuration. If you are using a config.xml file for your customization, place all of your customizations in the file and do not use Windows Installer public properties at the same time.

Global Customizations (FastPath Replacement)

There are several configuration options which are not tied to a profile and change the fundamental behavior of the application. These configuration options are specified in the global_customizations section of the file.

XML Comments explaining each customization are shown in red.

```
<?xml  version="1.0" encoding="iso-8859-1"?>
<agnclient>
        <global_customizations>
            <!-- Means that the Save Password checkbox will be hidden -->
                < flag name="HideSavePassword" value="Y" />
            <!-- Means that the Save Password checkbox will be checked by default -->
                <flag name="DefaultSavePasswordOn" value="Y" / >
            <!-- Means that the Pin and Token is shown and not the password field -->
                <flag name="InitiallyShowPinAndToken" value="N" / >
            <!-- Means Browsers will not get any definitions from Service Manager -->
            <!-- This includes proxies so only use if you really know what is going on -->
                <flag name="DisableProgramUpdates" value="N" />
            <!-- Show all Wi-Fi hotspots by default - Service Manager settings will trump
                this setting after connecting the first time -->
        </global_customizations>
</agnclient>
```

Figure 33: Fastpath Replacement Configuration File Example

Trusted Domain Customization

The Trusted Domain Customization allows Customer Account Administrators to define a list of trusted domain suffixes at installation time. When the AT&T Global Network Client with the AT&T Global Network Client Firewall component is installed using a Trusted Domain list, the firewall is enabled by default unless the workstation is actively connected and assigned a Connection-specific DNS Suffix in the Trusted Domain list. This customization is commonly used for mobile laptop users that transition between public networks and a trusted Intranet office environment. The Trusted Domain Customization defines the trusted Intranet environment when the AT&T Global Network Client Firewall may inhibit productivity or prevent remote management tools from functioning properly.

The list is defined at installation time and once the trusted domains have been configured, there is no method to dynamically update them.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

There is one exception to the Trusted Domain Configuration; regardless of the Connection-specific DNS Suffix, if a VPN session is established the firewall is enabled on all interfaces.

Trusted Domain Configuration

The Trusted Domain Customization uses a Windows Installer public property to specify the list of Trusted Domains. Set the TRUSTED_DOMAINS Windows Installer public property to a comma delimited list of domain suffixes you want to be trusted when the installation package is deployed to your workstations. See the Advanced Customizations Using Windows Installer section on page 48 for examples of using Windows Installer public properties.

Trusted Domain Customization Limitations

The Trusted Domain Customization is an install time only configuration and cannot be updated on demand. There is one exception to the Trusted Domain Configuration; regardless of the Connection-specific DNS Suffix assigned, if a VPN session is established the firewall is enabled on all interfaces.

Client Profiles Customization

The Client Profiles Customization allows customer account administrators to define a list of client profiles at installation time. When the AT&T Global Network Client is installed using a Client Profile list, the client profiles are created at installation time rather than manually by the user after installation.

The list is defined at installation time and once the profiles have been configured, there is no method to dynamically update them.

Client Profiles Configuration File

The Client Profiles Customization requires a Configuration File be present during AT&T Global Network Client installation. The name of the configuration file must be defined via the **CONFIG_FILE** public property of the installation package (see the chapter on Customizations for more information on public properties of the AT&T Global Network Client). The Trusted LAN, Trusted Domain customization and Client Profiles Customization can be defined in the same configuration file.

The Configuration file uses the standard XML file format. The Client Profiles information is specified with three "tables" definitions for each profile, **"Profile"**, **"User"**, and **"ConfigSettings"** starting at 2001 for the first profile and increments by 1 for each additional profile (or instance of the heading, with some profiles more than one **"User"** may be required).

A **"Bookmark"** table heading identifies which of the profiles is the default profile. **SZLNKPROFILE** in the **"Bookmark"** section should be set to the **RECID** of the **"Profile"** you would like to be the default.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Specific values in each heading (**RECID, LNKUSER, LNKPROFILE, FLGSZNAME, …**) are required and should not be changed. Required values are shown in bold in the example below.

In the example below **Profile 2001, User 2001**, define a basic profile. **SZNAME** defines the name of the profile.

- **SZACCOUNT** defines the AT&T account of the user
- **SZUSERID** defines the AT&T user ID

It is recommended you do not customize profile properties that are configurable using the AT&T administration server (such as network service). Because of the ability to update the value at connect time, it is recommended to use the AT&T administration server to centrally define values when possible.

Following is an example of a Client Profile using all the public properties that might conflict with the "CONFIG_FILE" configuration file. Feel free to use this file and remove the sections you do not need:

XML Comments explaining some of the customizations are shown in red.

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!-- NOTE!!! This XML file has all the possibilities where there could be
 conflicts with PUBLIC PROPERTIES. You need to look at this XML and remove
 what is not appropriate to your installation -->
<agnclient>
        <!-- Old FastPath customizations are done here now -->
        <global_customizations>
                <!-- Means that the Save Password checkbox will be hidden -->
                <flag name="HideSavePassword" value="Y" />
                <!-- Means that the Save Password checkbox will be checked by default -->
                <flag name="DefaultSavePasswordOn" value="Y" />
                <!-- Means that the Pin and Token is shown and not the password field -->
                <flag name="InitiallyShowPinAndToken" value="" />
                <!-- Means Browsers will not get any definitions from Service Manager -->
                <!-- This includes proxies so only use if you really know what is going on -->
                <flag name="DisableProgramUpdates" value="" />
                <!-- Show all Wi-Fi hotspots by default - Service Manager settings will trump
                this setting after connecting the first time -->
        </global_customizations>
        <tables>
                <!-- Sets the default profile -->
                <table name="bookmark">
                        <record>
                        <!-- Linking to Profile 2001 defined lower -->
                        <lnkprofile>2001</lnkprofile>
                        <!-- Set profiles to be Internet Only or credentialess connections -->
                        <!-- this would be the INTERNET_ONLY=1 Public Property -->
                        <LnkAPConnection>401</LnkAPConnection>
                        <!-- Show the digital certificate checkbox on the User ID setup window -->
                        <!-- this would be the CERT_SHOW=1 Public Property -->
                        <ShowDigCertCheckbox>1</ShowDigCertCheckbox>
                        <!-- Check the digital certificate checkbox on the User ID setup window -->
                        <!-- this would be the CERT_SHOW=1 Public Property -->
                        <CheckDigCertCheckbox>1</CheckDigCertCheckbox>
                        </record>
                 </table>
                <table name="profile">
                        <!-- Define the default profile -->
                        <record>
                                <recid>2001</recid>
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

```
                                <!-- this would be the PROFILENAME Public Property -->
                                <szname>My Imported Profile</szname>
                                <!-- Linking to the User 2001 defined lower -->
                                <lnkuser>2001</lnkuser>
                                <!-- Default Service is 400 -->
                                <lnkprofile>400</lnkprofile>
                                <flgszname>1</flgszname>
                        </record>
                        <!-- Define the second profile -->
                        <record>
                                <recid>2002</recid>
                                <szname>My Second Profile</szname>
                                <!-- Linking to the User 2002 defined lower -->
                                <lnkuser>2002</lnkuser>
                                <extuser>2002</extuser>
                                <flgszname>1</flgszname>
                        </record>
                </table>
                <table name="user">
                        <record>
                                <!-- Linking to Profile 2001 defined above -->
                                <recid>2001</recid>
                                <!-- this would be the ACCOUNT= Public Property -->
                                <szaccount>Account1</szaccount>
                                <szuserid>MyUserId</szuserid>
                                <lnkuser>200</lnkuser>
                                <!-- Hide the Save Password checkbox on the Network Logon Screen -->
                                <!-- this would be the HIDE_SAVE_PASSWORD=1 Public Property -->
                                <hidesavepassword>Y</hidesavepassword>
                        </record>
                        <record>
                                <!-- Linking to Profile 2002 defined above -->
                                <recid>2002</recid>
                                <szaccount>Account2</szaccount>
                                <szuserid>MyUserId</szuserid>
                                <lnkuser>200</lnkuser>
                                <!-- Set the password  -->
                                <!-- this would be the PASSWORD= Public Property -->
                                <szencryptedpassword>mypassword</szencryptedpassword>
                        </record>
                </table>
        </tables>
</agnclient>
```

Figure 34: Client Profiles Configuration File Example

Creating Profiles to not Autoconnect

To create profiles that won't autoconnect after starting up, use the following example:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<agnclient>
        <tables>
                <!-- Sets the default profile -->
                <table name="bookmark">
                        <record>
                        <!-- Linking to Profile 2001 defined lower -->
                        <lnkprofile>2001</lnkprofile>
                        <LnkAPConnection>400</LnkAPConnection>
                        </record>
                  </table>
                <table name="profile">
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

```
                        <!-- Define the default profile -->
                        <record>
                                <recid>2001</recid>
                                <!-- this would be the PROFILENAME Public Property -->
                                <szname>My Imported Profile</szname>
                                <!-- Linking to the User 2001 defined lower -->
                                <lnkuser>2001</lnkuser>
                                <!-- Default Service is 400 -->
                                <lnkprofile>400</lnkprofile>
                                <flgszname>1</flgszname>

                <smusermayoverrideautoreconnectdefaults>Y</smusermayoverrideautoreconnectdefaults>
                                <overrideautoreconnectdefaults>Y</overrideautoreconnectdefaults>
                                <enablepersistentconnection>N</enablepersistentconnection>
                                <autoreconnectinternet>N</autoreconnectinternet>
                        </record>
                        <!-- Define the second profile -->
                        <record>
                                <recid>2002</recid>
                                <szname>My Second Profile</szname>
                                <!-- Linking to the User 2002 defined lower -->
                                <lnkuser>2002</lnkuser>
                                <extuser>2002</extuser>
                                <flgszname>1</flgszname>

                <smusermayoverrideautoreconnectdefaults>Y</smusermayoverrideautoreconnectdefaults>
                                <overrideautoreconnectdefaults>Y</overrideautoreconnectdefaults>
                                <enablepersistentconnection>N</enablepersistentconnection>
                                <autoreconnectinternet>N</autoreconnectinternet>
                        </record>
                </table>
                <table name="user">
                        <record>
                                <!-- Linking to Profile 2001 defined above -->
                                <recid>2001</recid>
                                <!-- this would be the ACCOUNT= Public Property -->
                                <szaccount>Account1</szaccount>
                                <szuserid>MyUserId</szuserid>
                                <lnkuser>200</lnkuser>
                        </record>
                        <record>
                                <!-- Linking to Profile 2002 defined above -->
                                <recid>2002</recid>
                                <szaccount>Account2</szaccount>
                                <szuserid>MyUserId</szuserid>
                                <lnkuser>200</lnkuser>
                        </record>
                </table>
        </tables>
</agnclient>
```

Other Commonly Requested Customizations

The following are some common configurations and customizations. The details of implementing these customizations are provided.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Network Login Option Customizations

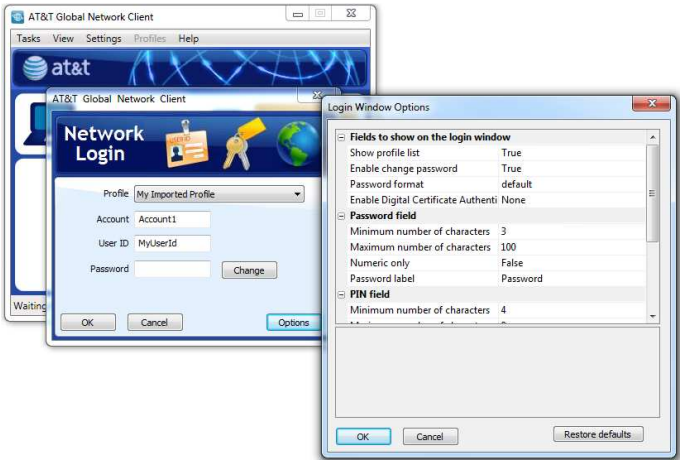


Figure 35: Network Login Options

Many customers need to set the options for the login properties dialog. The following is a list of customizations to add the CONFIG_FILE Public Property xml file:

Hide Options Button

```
<agnclient>
<registry_customizations>
        <registry type="string">
                <branch>HKEY_LOCAL_MACHINE\SOFTWARE\AGNS\NetClient\Settings\LoginOptions</branch>
                <field>HideOptionsLink</field>
                <value>1</value>
        </registry>
</registry_customizations>
</agnclient>
```

Use Digital Certificates

Value options are:
"1" for Use Local Store
"2" for Use Smart Card

```
<agnclient>
<registry_customizations>
        <registry type="string">
                <branch>HKEY_LOCAL_MACHINE\SOFTWARE\AGNS\NetClient\Settings\LoginOptions</branch>
                <field>UseDigitalCertificates</field>
                <value>1</value>
        </registry>
</registry_customizations>
</agnclient>
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Password Format

Value options are:
"1" for Regular Password
"2" for Pin and Token

```
<agnclient>
<registry_customizations>
        <registry type="string">
                <branch>HKEY_LOCAL_MACHINE\SOFTWARE\AGNS\NetClient\Settings\LoginOptions</branch>
                <field>PasswordFormat</field>
                <value>2</value>
        </registry>
</registry_customizations>
</agnclient>
```

Other Network Login Options

PasswordMinChars	To set the password minimum characters option. Any valid numeric can be used. (Default value is 3)
PasswordMaxChars	To set the password maximum characters option. Any valid numeric can be used. (Default value is 100)
PINMinChars	To set the PIN minimum characters option. Any valid numeric can be used. (Default value is 4)
TokenMinChars	To set the Token minimum characters option. Any valid numeric can be used. (Default value is 4)
PINMaxChars	To set the Pin maximum characters option. Any valid numeric value can be used. (Default value is 8)
TokenMaxChars	To set the Token maximum characters option. Any valid numeric can be used. (Default value is 8)
PasswordPrompt	To customize the text of the password label. Any valid text/string can be used. *Note: Making it too long will cut off text.*
PINPrompt	To customize the text of the PIN label. Any valid text/string can be used. *Note: Making it too long will cut off text.*

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Limiting Connections Per Operating System

If more than one range of Operating systems need to be defined, then the config.xml will have to be used instead of the LPE_OS_RANGE putblic property. The following example would allow Vista SP2, Windows 7 SP1 through Windows 8 Update 1.

```
<agnclient>
  <user_interface>
    <checkforos lowervalue="6.1.0002" uppervalue="6.1.0002" />
    <checkforos lowervalue="6.1.7601" uppervalue="9.9.9999" />
  </user_interface>
</agnclient>
```

See http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx for more information.

Profile Customization Limitations

The Client Profile Customization is an install time only configuration and cannot be updated on demand.

Controlling the AT&T Global Network Client Firewall

The state of the AT&T Global Network Client Firewall is "on", "off", or "disabled" and the initial state is set by specifying the **FIREWALL_STATE** public property. If it is set to "disabled" you must also request that your AT&T representative update your Firewall Setting in the AT&T Administration Server to "N".

NOTE: The FIREWALL_STATE public property sets the initial state only. Once the user connects to the network, this property may be overridden by the central firewall configuration downloaded from the AT&T Administration Server.

Network Awareness Customization

The Network Awareness customization provides the ability to define an AT&T Global Network Client action to be performed when a user connects to a defined network.

The following actions are currently supported using Network Awareness:

- No AT&T Global Network Client connection required, immediately disconnect the AT&T Global Network Client
- No AT&T Global Network Client connection required, immediately prompt the user to disconnect the AT&T Global Network Client
- Minimize the AT&T Global Network Client

When the user connects to a network defined to not require an AT&T Global Network Client connection, the AT&T Global Network Client connect button will be disabled.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Figure 36: Disabled Connect Button

If the user is connected to the internet and then connects to their corporate network, they can be prompted to disconnect their VPN session.

Figure 37: Prompt to Disconnect when Work Network is detected

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Defining Networks and Corresponding Actions

The Network Awareness customization requires central configuration; the Network Awareness field in the AT&T administration server must be set to "**Y**". Refer to Appendix A: Central Configuration for additional information about central configuration.

This customization requires you to define the network(s) by creating a NetworkAwarness.xml file. Working knowledge of XML is recommended to perform this customization. The NetworkAwarness.xml file is read when the AT&T Global Network Client is launched and any subsequent changes are not effective until the AT&T Global Network Client is shutdown and restarted. Please note that xml style comments are not supported in the file at this time.

The XML file must be found at the following path:

"%ALLUSERSPROFILE%\AGNS\NetClient\NetworkAwareness.xml"

Following is an example of a Network Awareness XML configuration file:

```
<network_location>
        <description>the AT&amp;amp;T network</description>
        <active>Y</active>
        <action>IMMEDIATELY_DISCONNECT</action>
        <action>MINIMIZE_CLIENT</action>
        <subnet>135.0.0.0,255.0.0.0</subnet>
        <subnet>129.1.0.0,255.0.0.0</subnet>
        <wins_server_list>2.2.2.2,3.3.3.3</subnet>
        <operator>OR</operator>
</network_location>
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

The table below defines the settings configurable using the NetworkAwareness.xml.

Stanza	Description
network_location	A brief description of network – this is displayed on the AT&T Global Network Client user interface so the name should be kept short to preserve readability. **ONLY ONE network_location stanza may be defined in the NetworkAwareness.xml file**.
Active	Set to "**Y**" for the AT&T Global Network Client to actively look for and perform an action for this network location. Set to "**N**" to perform no action.
Action	Set to one or more available actions: IMMEDIATELY_DISCONNECT PROMPT_TO_DISCONNECT MINIMIZE_CLIENT
Subnet	Set to one or more IP address/subnet mask combinations to define the network. Multiple subnets can be defined by repeating this stanza within the network location stanza.
dns_suffix_list	Set to DNS suffix to identify network location. Multiple suffix's can be defined by separating suffix's with a comma. Multiple suffixes within the list are combined using "**OR**".
dns_server_list	Set to DNS Server IP Addresses to identify network location. Multiple IP Address's can be defined by separating IP Address's with a comma. Multiple IP Addresses within the list are combined using "**OR**".
wins_server_list	Set to WINS Server IP Addresses to identify network location. Multiple IP Address's can be defined by separating IP Address's with a comma. Multiple IP Addresses within the list are combined using "**OR**".
Operator	Set to "**OR**" or "**AND**" to determine how to combine multiple types of identifiers (subnet,

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Stanza	Description
	dns_suffix_list, wins_server_list). Default: "**OR**"

Approved Mobile Device Customization

The Approved Mobile Device customization provides the ability to define a list of approved mobile devices with which your users can connect using the AT&T Global Network Client.

The following registry key is required:

HKLM\Software\AGNS\NetClient\WAN\AllowedDevices

The key must be created as a multi-string registry key at installation time. Multiple devices can be defined; each device should be listed on a separate line of the registry key. This is an allow list, only devices in the list will be supported.

The items in the list are compared against the installed mobile device model name for a match. If a match is not found, the user will receive a pop-up warning them the device cannot be used. The mobile icon will be disabled and mobile connection will have a status of **disabled** in the Connection Sequence window.

The AT&T Global Network Client must be restarted after the device is removed for the mobile icon to be enabled.

Approved Connection Type Customization

Beginning with Version 9.1, Customer Account Administrators can select to show or hide the Dial, Wi-Fi or Mobile connection types. Customizing the visibility of connection types requires a custom installation package created by AT&T. Please contact dl-AGNC_custom@att.com for additional information.

By default Ethernet/Existing, Wi-Fi and Mobile connection types are shown. Dial is not shown by default, but can be displayed by the end user. Dial, WiFi and Mobile connection types can be hidden through customization. Hiding a connection type will hide ALL subtypes of that connection type by default.

Connection Type Which Can Be Hidden
Dial
WiFi
Mobile

Secondary Method of Customizing Network Login Options

The fields and functionality of the Network Login window can be configured by clicking the "Options" button on the Network Login window. The Login Options window shows the features that can be configured.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

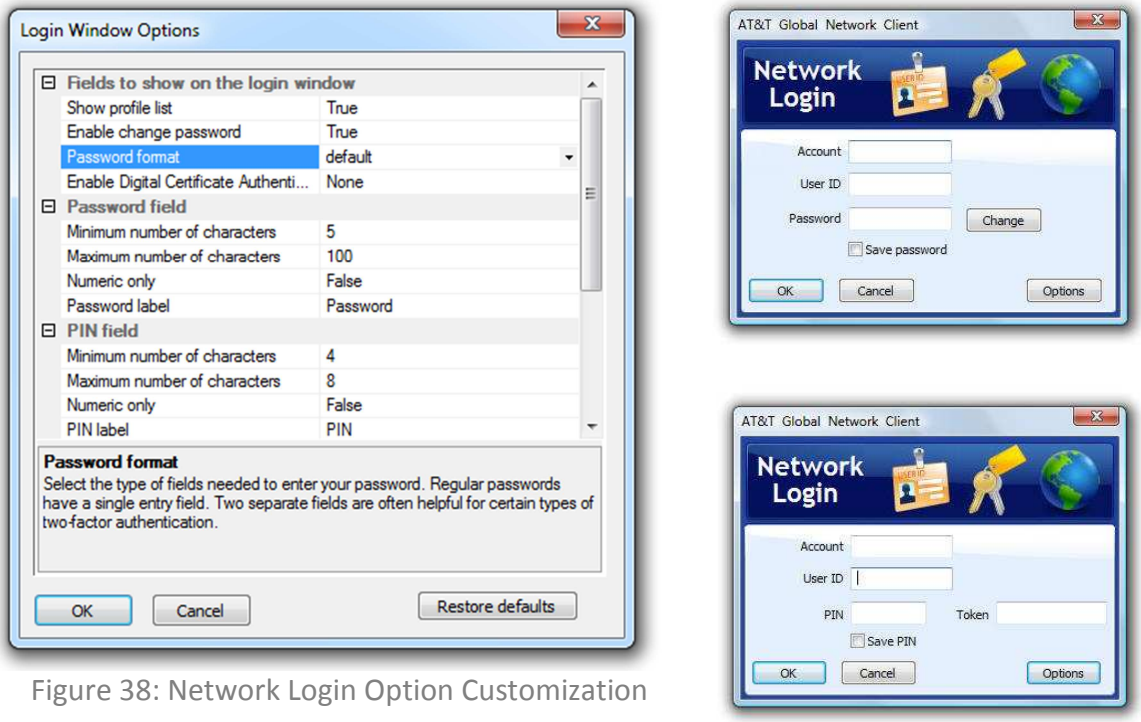


Figure 38: Network Login Option Customization

Customizing Default Login Options

The default login options can be customized by configuring them in the Windows registry. Default login options can be stored in the HKEY_LOCAL_MACHINE registry branch. User modified options are stored in the HKEY_CURRENT_USER registry branch and take precedence over the default values. (See the Hiding Login Options section for instructions on how to prevent users from changing the login options.)

Customizing Default Login Properties

1. Run the AT&T Global Network Client and configure the login options as desired.
2. Run regedit.exe and export the following branch to a file called LoginOptions.reg:
   HKEY_CURRENT_USER\Software\AGNS\NetClient\Settings\LoginOptions
   **Note: The branch will not exist until after the first login attempt.
3. Edit LoginOptions.reg and change HKEY_CURRENT_USER to HKEY_LOCAL_MACHINE.
4. Merge LoginOptions.reg into the registry to store the defaults.

Figure 39: Customizing Default Login Properties Table

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Customization Services

Customization services, including advanced customization support, can be supplied by AT&T. Dynamic and centrally managed customizations are available. Please contact your AT&T Account Representative for additional information. If they are not familiar with the customization services, have them refer to an AT&T Intranet site: https://olympus.labs.att.com/

SDK Prioritization

You are able to change the prioritization of the Windows Mobile Broadband SDK relative to other mobile SDKs.

Windows Mobile Broadband is only available in Microsoft Windows 7 and Windows 8.

The file is included under the "\AT&T Global Network Client\CellularPlugInController" directory. It is basically a list of SDK's in descending SDK priority:

```
<?xml version="1.0" encoding="utf-8"?>
<SDKPriorityList>
        <SDK name="COMGobiSDKServer.exe"/>
        <SDK name="COMSierraGSMSDKServer.exe"/>
        <SDK name="COMSierraCDMASDKServer.exe"/>
        <SDK name="COMSierraGobiSDKServer.exe"/>
        <SDK name="COMWMBServer.exe"/>
        <SDK name="COMSmartcomSDKServer.exe"/>
</SDKPriorityList>
```

Figure 40: SDK Prioritization

The file does allow you to make the WMB SDK a higher or lower priority than any SDK in the list. For example, if you want to make the WMB SDK a higher priority than all the SDKs except Sierra GSM, you could change the file as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<SDKPriorityList>
        <SDK name="COMSierraGSMSDKServer.exe"/>
        <SDK name="COMWMBServer.exe"/>
        <SDK name="COMGobiSDKServer.exe"/>
        <SDK name="COMSierraCDMASDKServer.exe"/>
        <SDK name="COMSierraGobiSDKServer.exe"/>
        <SDK name="COMSmartcomSDKServer.exe"/>
</SDKPriorityList>
```

Figure 41: SDK Prioritization Change Example

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Please note the file does not allow you to change the priorities of non-WMB SDKs relative to each other. Those stay fixed irrespective of any change done to the file.

Accessibility Features

The AT&T Global Network Client complies with US regulations to support accessibility for persons with disabilities, including Section 508 regulations.

Visual Display of Screen Element in Focus

The AT&T Global Network Client screen element in focus is depicted by a gray highlighted box surrounding the control. When first launched, the Connect button is in focus as shown below.

Figure 42: Main Window

Keyboard Navigation

The AT&T Global Network Client can be navigated and utilized exclusively using a keyboard.

The controls can be operated either by pressing the space bar or the Enter key.

To move between controls, use the tab key to navigate forward or shift key and tab key in unison to navigate backward. To simulate a right mouse click, use the menu key or the shift key in unison with the F10 key.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Extended Access

Extended Access is an AT&T service feature that allows remote users to access the network through local points of presence (PoPs) that are owned and managed by another Internet Service Provider (ISP) that is an AT&T partner. Extended Access provides local access in over 143 countries where AT&T does not have PoPs. There is an hourly access charge for the use of Extended Access – the amount of which is based on the region in which the Extended Access takes place.

The Extended Access ISP proxies users' authentication requests to AT&T to allow access to the Internet. The protocol and data flow for connecting to Extended Access PoPs vary depending on the service being accessed. For more information, go to the AT&T Extended Access web site at http://info.attbusiness.net/e-access.

Extended Access and AT&T Business Internet Service (BIS)

New AT&T customers registered in the United States and Canada that have signed an AT&T Master Agreement dated 10/21/02 or later, and existing customers that have previously signed an agreement that references the AT&T Business Internet Services Global Service Description are eligible to use the feature immediately. All other customers should contact their account representative.

Internet Extended Access Authentication Options

When connecting to an Extended Access PoP for AT&T Business Internet Service, Enhanced Authentication is typically used for the connection process

Extended Access and AT&T VPN Services (AT&T VPN Tunneling Services)

Contact your AT&T account representative to order this feature.

Your AT&T account representative gives the users' access to the extended PoPs by enabling the Extended Access field in the AT&T administration server.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T Lightweight Policy Enforcement

AT&T Lightweight Policy Enforcement (LPE) is an optional service available to AT&T customers using the AT&T Global Network Client for connectivity. AT&T Lightweight Policy Enforcement performs basic application monitoring and can be customized by the Customer Account Administrator at installation time.

Installation of the Lightweight Policy Enforcement feature is optional. Customer Account Administrators can use control Lightweight Policy Enforcement definitions using the XML CONFIG_FILE Public Property at installation time or the Windows Installer ADDLOCAL and REMOVE properties to control installation of the feature for all users. See the Customizations Chapter on page 48 of this guide for more information about installation customization.

Lightweight Policy Enforcement feature can also be used to monitor 3rd party VPN client.

Asset Based Connection Prevention

Beginning in 9.6, connections can be prevented based on

- Operating System/Service Packs
- A specified file
- A registry hive in HKEY_LOCAL_MACHINE

Operating System

Allow range of Operating Systems to be used

With the AGNC_LPE_OS_RANGE public property, the lowest allowed, highest allowed, or lowest and highest together. For

Allow range of Operating Systems to be used

To prevent connections based on obsolete or unsupported Operating Systems or Service Packs, you can do so by using the Public Property, LPE_OS_RANGE at install time. By specifying the numeric value range of the Operating System, connections will not be allowed. For example, if the company policy is to prevent connections on Windows Vista, you would specify:

LPE_OS_RANGE=6.0.6000-6.0.6002

6.0.6000 is Vista RTM and 6.0.6002 is Vista Service Pack 2.

For more information on Operating System build numbers, see http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx

For multiple ranges, the config file should be used instead of public properties.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Specified File

To prevent connections based on whether a specific file exists on the user's system, use the LPE_FILE Public Property at install time. If the specified file does not exist, then a connection will not be allowed.

Registry hive in HKEY_LOCAL_MACHINE

To prevent connections based on whether a specific file exists on the user's system, use the LPE_REG Public Property at install time. If the specified registry hive does not exist, then a connection will not be allowed. For example, if you have company defined asset information entry in the HKEY_LOCAL_MACHINE hive**,** that would not be on a non-asset system, you can use that information to prevent a connection, e.g. LPE_FILE="SOFTWARE\MyCompany\Asset\Identifier"

Application Monitoring

The application monitor feature allows a Customer Account Administrator to specify configuration policies to monitor antivirus programs, firewalls, anti-spyware programs and VPN clients for remote-access connections connected with the AT&T Global Network Client. The rules are configured through a custom kit. Some basic Lightweight Policy Enforcement rules can be enforced by a using the XML based CONFIG_FILE Public Property at installation time.

A threshold value indicating the number of failed compliance checks allowed before the AT&T Global Network Client performs the compliance failure action can be configured by the Customer Account Administrator through customization. See the LPE_COMPLIANCE_THRESHOLD public property in the chapter on Customizations for more information.

When VPN monitoring rules are created, if the monitored VPN client disconnects from the VPN server, the AT&T Global Network Client will likewise disconnect the remote access connection.

Types of Applications Monitored

Pre-defined antivirus, firewall, anti-spyware and VPN applications can be monitored. The following table shows the types of applications that can be monitored, as well as what is monitored.

Application Type	Items Monitored
Firewall	• Whether Process is Running • Product Version
Anti-Virus	• Whether Process is Running • Product Version • Virus Definition File Timestamp
Anti-Spyware	• Whether Process is Running • Product Version • Anti-Spyware Definition File Timestamp
VPN	• Whether client is connected or not

For a complete list of applications see the web site at http://www.corp.att.com/agnc.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

The Lightweight Policy Enforcement firewall monitoring is used to determine if a firewall is enabled prior to checking for and connecting to free Wi-Fi hotspots. The AT&T Global Network Client will allow the association to potentially free hot spots if any known firewall is running, thus allowing customers to use their own corporate or personal firewall software instead of the AT&T provided firewall.

Limitations

The application monitoring rules are determined at installation time and cannot be dynamically updated. If a user is out of compliance with the policy, the connection is rejected. The user is given a generic error message. The user must make the necessary changes to return to compliance with the policy manually, and without a connection using the AT&T Global Network Client.

Lightweight Policy Enforcement Customization Examples

The AT&T Global Network Client Lightweight Policy Enforcement Customization allows customers to create their own enforcement policy using the CONFIG_FILE public property.

Using CONFIG_FILE Public Property with XML

To set the Lightweight Policy Enforcement for the login properties dialog. The following is a list of customizations to add the CONFIG_FILE Public Property xml file:

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

LPE for a Generic Firewall

```
<agnclient>
<lpe_rules>
        <!-- check for any FireWall running before connecting with the AT&T Global
Network Client -->
        <rule_group when="before_connecting" id="RequireFw" poll_frequency="60"/>
        <!-- check for any FireWall running AFTER connecting with the AT&T Global
Network Client, Check every 60 seconds -->
        <rule_group when="after_connecting" id="RequireFw" poll_frequency="60"/>
</lpe_rules>
</agnclient>
```

LPE for a Generic Anti-Virus

```
<agnclient>
<lpe_rules>
        <!-- check for any Anti-Virus running before connecting with the AT&T Global
Network Client -->
        <rule_group when="before_connecting" id="RequireAv" poll_frequency="60"/>
        <!-- check for any Anti-Virus running AFTER connecting with the AT&T Global
Network Client, Check every 60 seconds -->
        <rule_group when="after_connecting" id="RequireAv" poll_frequency="60"/>
        <!-- Update dats silently if older than 5 days -->
        <rule_group when="before_connecting" id="RequireFwAvUpdateIf5DaysOld"
poll_frequency="60" />
</lpe_rules>
</agnclient>
```

Lightweight Policy Enforcement for Generic Anti-Virus package or Firewall not running.

```
<?xml version="1.0" encoding="iso-8859-1"?>
<agnclient>
<tables>
        <table name="appmonstate">
                <record>
                        <!-- Rule ID = FW is running -->
                        <groupid>210</groupid>
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

```
                <state>1</state>
                <ruleid>201</ruleid>
                <!-- Process next rule -->
                <passnextstate>2</passnextstate>
                <failnextstate>0</failnextstate>
                <!-- FailAction 1 is to Disconect -->
                <failaction>1</failaction>
                <!-- Generic Message for Firewall -->
                <failmessage>6472</failmessage>
        </record>
        <record>
                <groupid>210</groupid>
                <state>2</state>
                <ruleid>202</ruleid>
                <!-- Rule ID = Any Anti-Virus is running -->
                <passnextstate>0</passnextstate>
                <failnextstate>0</failnextstate>
                <!-- FailAction 1 is to Disconect -->
                <failaction>1</failaction>
                <!-- Customized Message for Anti-Virus -->
                <failmessage>6474</failmessage>
        </record>
</table>
<table name="appmonrule">
        <record>
                <!-- 201 is first rule to use-->
                <ruleid>201</ruleid>
                <!-- 0 = is running-->
                <type>0</type>
                <!-- 7 = "NONE" -->
                <expression>7</expression>
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

```
                    <!-- Make sure there is some Firewall running -->

        <program>pn=AgnAnyFirewall,pv=none,pt=fw,pi=none,datver=n,dattime=n</program>
                    <operand></operand>
                </record>
                <record>
                    <!-- 202 is second rule to use-->
                    <ruleid>202</ruleid>
                    <!-- 0 = is running-->
                    <type>0</type>
                    <!-- 7 = "NONE" -->
                    <expression>7</expression>
                    <!-- Make sure there is some Anti-Virus running -->

        <program>pn=AgnAnyAntiVirus,pv=none,pt=av,pi=none,datver=n,dattime=y</program>
                    <operand></operand>
                </record>
        </table>
</tables>
<lpe_rules>
        <rule_group when="before_connecting" id="210" poll_frequency="60"/>
        <!-- Check every 60 seconds or once a minute after connecting -->
        <rule_group when="after_connecting" id="210" poll_frequency="60"/>
</lpe_rules>
</agnclient>
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Example: Display a warning message for a generic Anti-Virus package and disconnect if not running the Microsoft Windows Firewall.

```
<?xml version="1.0" encoding="iso-8859-1"?>
<agnclient>
<user_interface>
        <module name="NetClientDll" moduleid="2">
        <!-- Modify the message from disconnected to a warning -->
        <resource name="NetClientDll" resourceid="6474" value="Please start your Anti-Virus
program now."/>
        </module>
        </user_interface>
<tables>
        <table name="appmonstate">
                <record>
                        <!-- Rule ID = Windows FW is running -->
                        <groupid>211</groupid>
                        <state>1</state>
                        <ruleid>201</ruleid>
                        <!-- Process next rule -->
                        <passnextstate>0</passnextstate>
                        <failnextstate>0</failnextstate>
                        <!-- FailAction 1 is to Disconect -->
                        <failaction>1</failaction>
                        <!-- Generic Message for Firewall -->
                        <failmessage>6472</failmessage>
                </record>
                <record>
                        <groupid>210</groupid>
                        <state>1</state>
                        <ruleid>202</ruleid>
                        <!-- Rule ID = Any Anti-Virus is running -->
                        <passnextstate>0</passnextstate>
                        <failnextstate>0</failnextstate>
                        <!-- FailAction 4 is to Display Warning Msg -->
                        <failaction>4</failaction>
                        <!-- Customized Message for Anti-Virus -->
                        <failmessage>6474</failmessage>
                </record>
        </table>
        <table name="appmonrule">
                <record>
                        <!-- 201 is first rule to use-->
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

```
                        <ruleid>201</ruleid>
                        <!-- 0 = is running-->
                        <type>0</type>
                        <!-- 7 = "NONE" -->
                        <expression>7</expression>
                        <!-- Define particular Package -->
                        <program>pn=Microsoft Windows Firewall,pv=y,pt=fw,vn="Microsoft
Corp.",pi=MSWindowsFW,p3=,datver=n,dattime=n</program>
                        <operand></operand>
                </record>
                <record>
                        <!-- 202 is second rule to use-->
                        <ruleid>202</ruleid>
                        <!-- 0 = is running-->
                        <type>0</type>
                        <!-- 7 = "NONE" -->
                        <expression>7</expression>
                        <!-- Define particular Package -->
        <program>pn=AgnAnyAntiVirus,pv=none,pt=av,pi=none,datver=n,dattime=y</program>
                        <operand></operand>
                </record>
        </table>
</tables>
<lpe_rules>
        <rule_group when="before_connecting" id="211" poll_frequency="60"/>
        <!-- Check every 3600 seconds or once an hour after connecting -->
        <rule_group when="after_connecting" id="210" poll_frequency="3600"/>
</lpe_rules>
</agnclient>
```

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T Global Network Client Firewall

The AT&T Global Network Client Firewall is a component of the AT&T Global Network Client which provides basic firewall capabilities. The AT&T Global Network Client Firewall uses the Windows firewall engine for the firewall and fencing.

The AT&T Global Network Client Firewall provides the following:

- Blocks unsolicited traffic when not connected
- Blocks unsolicited Internet traffic while VPN connected

Overview

The AT&T Global Network Client Firewall is designed to protect a computer as a network firewall. The AT&T Global Network Firewall is turned off by default.

If it is turned on, either by the end user while not connected, or through central configuration via the AT&T Service Manager, the AT&T Global Network Client Firewall is active on all network card interfaces and all Microsoft Remote Access Services WAN/Dial-Up Networking interfaces whenever the workstation is powered on, regardless of whether there is a current connection to an AT&T network.

The AT&T Global Network Client Firewall monitors IP traffic; if an IP packet received is determined to be unsolicited[6] by the workstation, it is silently discarded. The AT&T Global Network Client Firewall does not perform any user notification of unsolicited traffic. If your computer did not request, negotiate, or grant permission for a connection with another machine, the traffic is silently rejected.

The AT&T Global Network Client Firewall also protects VPN sessions controlled by the AT&T integrated VPN client. Account administrators define their VPN network resources using an Access Control List (ACL) (AKA 'down the tunnel' network resources) in the AT&T Administration Server. Only traffic destined to one of the defined ACL resources is routed through the VPN tunnel. A setting in the AT&T Administration Server controls if non-VPN traffic should route over the Internet or be silently discarded.

OPSWAT Certified Firewall

The AT&T Global Network Client Firewall is certified through the OPSWAT Certification Program. This certification demonstrates that the AT&T Global Network Client Firewall is compatible with products from other market-leading technology vendors. Products carrying OPSWAT certification follow standards that indicate they will not adversely affect other installed security software. To learn more, visit the OPSWAT Certification website at http://www.opswat.com/certified

[6] The AT&T Global Network Client Firewall monitors new solicitation status as well as tracking port and SYNC status for current and expired sessions.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Operating Modes

The AT&T Global Network Client Firewall supports three operating modes. Certain modes require configuration in the AT&T administration server. Refer to Appendix A of this guide for more information about configuration options stored in the AT&T administration server. AT&T Global Network Client Firewall values set in the AT&T administration server always take precedence over values set locally using the AT&T Global Network Client.

Default

The Default configuration disables the firewall at all times, on all network interfaces.

Trusted Domains

The Trusted Domain configuration is used to control the firewall state for trusted domains. The Trusted Domain configuration enables the firewall at all times on all network interfaces unless it is actively connected and assigned a Connection Specific DNS suffix in a Trusted Domain list defined at installation time. Even in Trusted Domain mode, regardless of the Connection Specific DNS Suffix assigned, if an AT&T Integrated VPN session is established the firewall is enabled on all interfaces. See page 62 for more information on configuration of a Trusted Domain list.

User Controlled

The state of the firewall is controlled using the AT&T Global Network Client Firewall Settings Window described in the section below. This mode will be affected by the values set for **'Enable AT&T Global Network Client Firewall'** and **'User Controlled Firewall'** fields in the AT&T administration server.

Disabled

The Disabled configuration disables the firewall at all times, on all adapters. The user does not have the ability to turn the firewall on at any time.

When the user selects the **AT&T Global Network Client** from the **Start** menu, and clicks **Firewall Settings Window** the user will receive a message stating **"Your network administrator has chosen not to use the firewall."**

This mode requires a **"NO"** value set for **'Enable AT&T Global Network Client Firewall'** and **'User Controlled Firewall'** fields in the AT&T Administration Server.

Firewall Settings Window

The AT&T Global Network Client Firewall Settings Window allows a user to select the Firewall state (On/Off) when a VPN connection is not active. When the user establishes an active AT&T Global Network Client VPN connection the firewall is automatically enabled on all network interfaces unless the AT&T Global Network Client Firewall is operating in Disabled mode.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

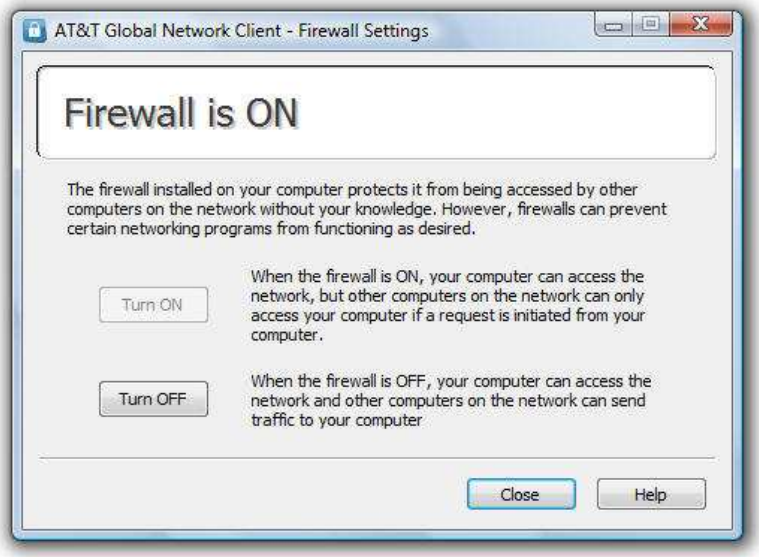

AT&T Global Network Client - Firewall Settings
Firewall is ON
The firewall installed on your computer protects it from being accessed by other computers on the network without your knowledge. However, firewalls can prevent certain networking programs from functioning as desired.
Turn ON
When the firewall is ON, your computer can access the network, but other computers on the network can only access your computer if a request is initiated from your computer.
Turn OFF
When the firewall is OFF, your computer can access the network and other computers on the network can send traffic to your computer
Close
Help

Figure 43: Firewall Settings Window

Allowing a user to turn the AT&T Global Network Client Firewall off when not VPN connected may be useful in environments that use enterprise management software to manage computers on a customer LAN since the firewall prevents the management software from having unsolicited access to the target machine.

The AT&T Global Network Client Firewall Settings window can be accessed by clicking the Microsoft Windows **Start** Menu, mouse over **All Programs**, click **AT&T Global Network Client**, and click **Firewall Settings**. The **Firewall Settings** application can only be open when the AT&T Global Network Client application is not running.

Customer Account Administrators can customize their AT&T Global Network Client installation to prevent the **Firewall Settings** window from being installed. Refer to the Customizations Chapter on page 48 of this guide for more information.

Whether users can modify the options on the **Firewall Settings** window can be controlled through the **'User Controlled Firewall'** setting in the AT&T Administration Server. When the **'User Controlled Firewall'** setting is set to **'N'**, the radio buttons on the Firewall Settings Window will be disabled and the user may view, but not change, the current state of the AT&T Global Network Client Firewall. Refer to Appendix A on page 103 of this guide for additional information about settings available in the AT&T administration server.

Managed VPN Access Control Lists

The only exceptions to the static firewall policy of denying all unsolicited traffic exist when there is an active Managed VPN Service connection. When VPN connected, the firewall does not block VPN traffic. With an active VPN connection, users receive all VPN traffic, solicited or unsolicited. Administrators have the ability to define an Access Control List (ACL) identifying the hosts with which a user can communicate through the VPN. Then the user can only initiate communication to those hosts defined in the Access

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Control List. If an Access Control List is not defined, all traffic is considered VPN traffic. Administrators can also define an Access Control List for their non-VPN interfaces (aka Internet interface). This is known as the Fenced Internet Access Control List.

Limitations

Beyond the Trusted Domain Customization, the AT&T Global Network Client Firewall policy cannot be customized by the Customer Account Administrator.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AT&T VPN Services

AT&T offers several advanced VPN services. The information in this chapter represents the most common administration and configuration questions.

Using Managed IPSec VPN Services

The security rules of the Managed VPN Services may require additional configuration or specific configuration settings to support your network infrastructure.

Local Resources

Accessing Local Resources

To access local resources (such as printers and other servers) outside the tunnel while a VPN tunnel is established, you must be using a VPN Dual Access capable service. VPN Dual Access allows you to access destinations outside the tunnel either locally or through the Internet in addition to resources down the tunnel.

Customer Account Administrators have the option to allow users that are not configured for Dual Access to access resources on their directly connected subnet by updating the **'Local Subnet Access'** to **'y'** at either the account or client-id level in the AT&T administration server. When the Local Subnet Access flag is set to yes and you are connecting with a non-dual access type service, the AT&T Global Network Client will determine the local subnet and set up the routing/rules to allow access to the local subnet.

Sharing Local Resources

You will not be able to host shared resources on the local LAN (such as printers) when a VPN tunnel is established. This traffic will be viewed as unsolicited IP traffic, and will be silently discarded by AT&T Global Network Client Firewall. The AT&T Global Network Client Firewall must be disabled via the AT&T administration server to support local resource sharing while VPN connected.

Registering VPN IP Address with Dynamic DNS

The AT&T Global Network Client can dynamically register an IP address in DNS when VPN connected regardless of the VPN server type. After VPN connected, the AT&T Global Network Client will gather the domain name, host name, and IP address then send out registration requests to all of the DNS servers in the VPN Adapter interface's DNS server list. To set this option, click **Show the login properties window.** from the **Settings** panel on the main window, click the **Preferences** tab, click **Override Defaults**, scroll down and click **Register VPN connection's address in DNS.** in the **VPN Details** section. If you have opted to turn off DNS registration through the network control panel, then the AT&T Global Network Client will not send the DNS update requests.

If the DNS server is configured for 'Secure Updates Only' and integrated with Active Directory, then the AT&T Network Logon Extensions component is required.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Encryption for IPSec VPN connections

Encryption can be configured in the AT&T administration server at the user account lever or sub account level. If values are specified in the AT&T administration server they will override the AT&T Global Network Client's default proposal behavior. Multiple algorithms can be selected, but the highest supported encryption level will always be proposed first.

Co-existence with Microsoft IPSec

Microsoft IPSec can be used for corporate protection strategies like Domain Isolation, Server Isolation, and IPSec based Network Access Protection (NAP) while VPN connected with the AT&T Global Network Client. Microsoft IPSec traffic travels through an AT&T VPN tunnel. No configuration changes are required when VPN tunneling with SSL-T services using the AT&T Global Network Client. If you are using Version 9.3 or later, no configuration changes are required when using IPSEC either, as the client will now default to use ephemeral source ports.

For IPSec services, the **Use Ephemeral IPSec Ports Login Properties** preference must be enabled. When enabled, the AT&T Global Network Client will NOT stop Microsoft's IPSec service and will use ephemeral source ports (1024+). This enables Microsoft to have sole ownership of IPSec source ports 500 and 4500.

This options is enabled by default. If the end user is having difficulty connecting, and you suspect the use of ephemeral source ports may be causing the issue, you can disable this option. To disable this option, click **Show the login properties window** from the **Settings** panel on the main window, click the **Preferences** tab, click **Override Defaults**, scroll down and deselect **Use ephemeral source ports for IPSec** in the **VPN Details** section.

NAT Traversal

The AT&T Global Network Client IPSec implementation supports NAT traversal through UDP encapsulation of IPSec traffic.

The NAT traversal implementation varies based on tunnel endpoint as listed below:

Cisco®[7] and AT&T Branded Tunnel Endpoints

NAT devices are auto-detected through a series of hashes during IKE negotiations. The AT&T VPN client uses UDP port 4500 as the source port and UDP port 4500 as the destination port in IKE negotiations and ESP IPSec data flows.

This implementation is based off the following Internet drafts:
http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-02.tx

Configuring UDP Encapsulation

A preference labeled **Negotiate UDP Encapsulation with VPN server for NAT Traversal** is available in the Login Properties/Preferences panel to allow an end user to alter the use of NAT Traversal. The default value for this preference can be centrally configured in the AT&T administration server, but can be

[7] Cisco is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

overridden by a user. To utilize NAT Traversal, this preference must be selected along with configuring the NAT Traversal settings on the VPN endpoint.

The AT&T Global Network Client client supports most NAT devices. There are known difficulties when tunneling IPSec traffic through NAT/firewalls which are documented in the following RFC http://www.ietf.org/rfc/rfc3715.txt.

AT&T is committed to supporting all NAT device vendors that are aware of the known IPSec compatibility issues and comply with the industry standards.

Cisco Passwords

If your network logon password has expired as determined by the authentication flows between the Cisco tunnel server and the Windows Primary Domain Controller, the AT&T Global Network Client will display a prompt for you to enter a new password. The VPN negotiation code will complete the change password exchange.

Using Managed SSL VPN Services

Managed SSL VPN is a client based tunneling solution. Managed SSL VPN traverses customer site proxies and firewalls without requiring network configuration changes. Fenced Internet hosts can be specified when tunneling with SSL-T dual access from a private line location.

Managed SSL VPN Services use TCP port 443 for authentication and tunneling. Alternatively, TCP port 80 can be used by unchecking the **Authenticate with HTTPS** preference in the AT&T Global Network Client **Login Properties**. Managed SSL VPN is successful because unlike IPSec, TCP port 443 can be passed through a proxy. The AT&T Global Network Client can be configured for proxy settings specific to connections using the AT&T Global Network Client using **Setup Wizard** or **Login Properties**, or the AT&T Global Network Client can use Microsoft Windows Internet Options proxy settings.

Network Layer Solution

Unlike some SSL solutions, Managed SSL VPN is a network layer solution. Therefore, all IP based applications (File Sharing/Outlook Exchange/VOIP/etc) are supported. Additionally, customer account administrators can access end user systems for software pushes, ad hoc message, etc. just as if their end users were residing on the Company's private local LAN.

Being VPN connected from behind a customer site proxy presents an extra layer of complexity for web-based applications such as a browser. By default, web-based applications will send all traffic directly to the proxy. However, Private LAN (VPN) and Local LAN traffic need to be routed differently. The AT&T Global Network Client enables a user to configure Internet Options for each specific proxy location to handle web-based applications correctly.

Security/Authentication

The Managed SSL VPN service use AT&T authentication server based authentication. The AT&T SSL VPN Server dictates the encryption method and currently enforces 3 DES and SHA-1. The AT&T SSL VPN Server is configured with an Entrust Server Certificate, and the AT&T Global Network Client utilizes Microsoft

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Internet Explorer's root certificate. When a TCP disconnect is detected, the AT&T Global Network Client will reestablish the session without user interaction.

Configuring the AT&T Global Network Client to Establish a VPN Connection through a Proxy

The AT&T Global Network Client performs these steps in the following order when establishing a VPN connection during the initial authentication request:

1. Attempt to connect directly across the existing network connection.
2. Attempt to connect using the user specified proxy information for this location, if specified.
3. Attempt to connect using the Microsoft Operating System (Internet Explorer) supplied proxy information.

The AT&T Global Network Client User's Guide contains detail instructions on configuring the proxy in the AT&T Client, through the Microsoft operating system, and the browser.

Importing a Proxy File for SSL connections

You have the option of using a proxy.ini file to configure browser settings specific to the proxy location you are visiting so you can access your corporate network through your SSL connection. The proxy settings are used by the AT&T Global Network Client to authenticate and establish the connection to your private network.

Proxy.ini File

You will need to provide your users with the proxy.ini file. Proxy information entries are configurable in the "proxy.ini" file located in the \Program Files\AT&T Global Network Client directory. One or more proxy information entries can be configured in the "proxy.ini" file. Below is a sample proxy.ini file.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

```
[CompanyXYZ]
default=yes
ProxyAddress=1.2.3.4
ProxyPort=8000
UserName=
Password=
AuthType=0

[CompanyZYX]
default=no
ProxyAddress=4.3.2.1
ProxyPort=9000
UserName=
Password=
AuthType=0
…
```

Figure 44: Proxy.INI File Example

proxy.ini Field Information:

default - If yes, and the AT&T Global Network Client could not connect through a direct network connection, an attempt to connect will automatically be made by the AT&T Global Network Client to establish a VPN connection with this Proxy Information. Only one entry should be specified as the default entry if multiple entries exist in the proxy.ini file.

ProxyAddress – IP Address of the proxy. This cannot be an auto proxy url.

ProxyPort – Port used to connect to the proxy.

UserName – Used for Proxies that require authentication. (this can be left blank and the user will be prompted later)

Password – Used for Proxies that require authentication. (this can be left blank and the user will be prompted later)

AuthType – 0 indicates the proxy does not require authentication.
1 indicates the proxy requires authentication

Importing the Proxy.ini file

To import your proxy.ini file, use the Settings and Proxy Settings menu.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Figure 45: Proxy Settings Menu

Switching to IPSec Over Dial Connections

If your company prefers using IPSec protocol whenever possible, the AT&T Global Network Client can be configured to use IPSec for dial connections.

This option requires central configuration and configuration in the AT&T Global Network Client. You must be authorized for both SSL and IPSec services in the AT&T administration server. To configure this option in the AT&T Client, click **Settings** menu; then **Login Properties**. Click the **Preferences** tab; click **Override Defaults;** scroll down and click **Switch from SSL to IPSec over dial connections** in the **VPN Details** section.

Dynamically VPN Connect

For companies who want users to VPN connect behind a proxy server, the AT&T Global Network Client can dynamically detect a proxy server in the network path and VPN connect using Transparent Tunneling (SSL-T). With this feature you can roam from a non-proxy site to a proxy site and not have to manually change any settings on the AT&T Global Network Client. This option only works with AT&T VPN Servers (VIG/SIG/Gateway) terminating the connection.

This option requires central configuration and configuration in the AT&T Global Network Client. You must be authorized for both SSL and IPSec services in the AT&T Administration Server and the **SSL AT&T Global Network Client Allow Proxy** setting must be set to **Y** in the AT&T administration server. To configure this option in the AT&T Client, click **Settings** menu; then **Login Properties**. Click the **Preferences** tab; click **Override Defaults**; scroll down and click **Use SSL Tunneling when a proxy server is detected** in the **VPN Details** section.

If your company prefers to use IPSec, but would like a failover service that will traverse more network paths, the AT&T Global Network Client can dynamically failover to Transparent Tunneling (SSL-T) service if the IPSec connection fails for any reason. In the AT&T administration server, set the **AT&T Global**

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Network Client IPSec Failover setting to **Y**. To configure this option in the AT&T Global Network Client, click **Settings** menu; then **Login Properties**. Click the **Preferences** tab; scroll down and click **Use SSL Tunneling when an IPSec connection cannot be established** in the **VPN Details** section.

IPv6 Support

Support for the following IP version tunneling scenarios is available when using IPSec or SSL-T VPN terminating to an AT&T VPN Server (SIG or VIG):

- IPv6 over IPv4
- IPv6 and IPv4 over IPv4
- IPv4 over IPv6
- IPv4 and IPv6 over IPv6

Tunneling is automatic and transparent to the user. IP Address configuration occurs during tunnel setup when the VPN server assigns the VPN Client address(s).

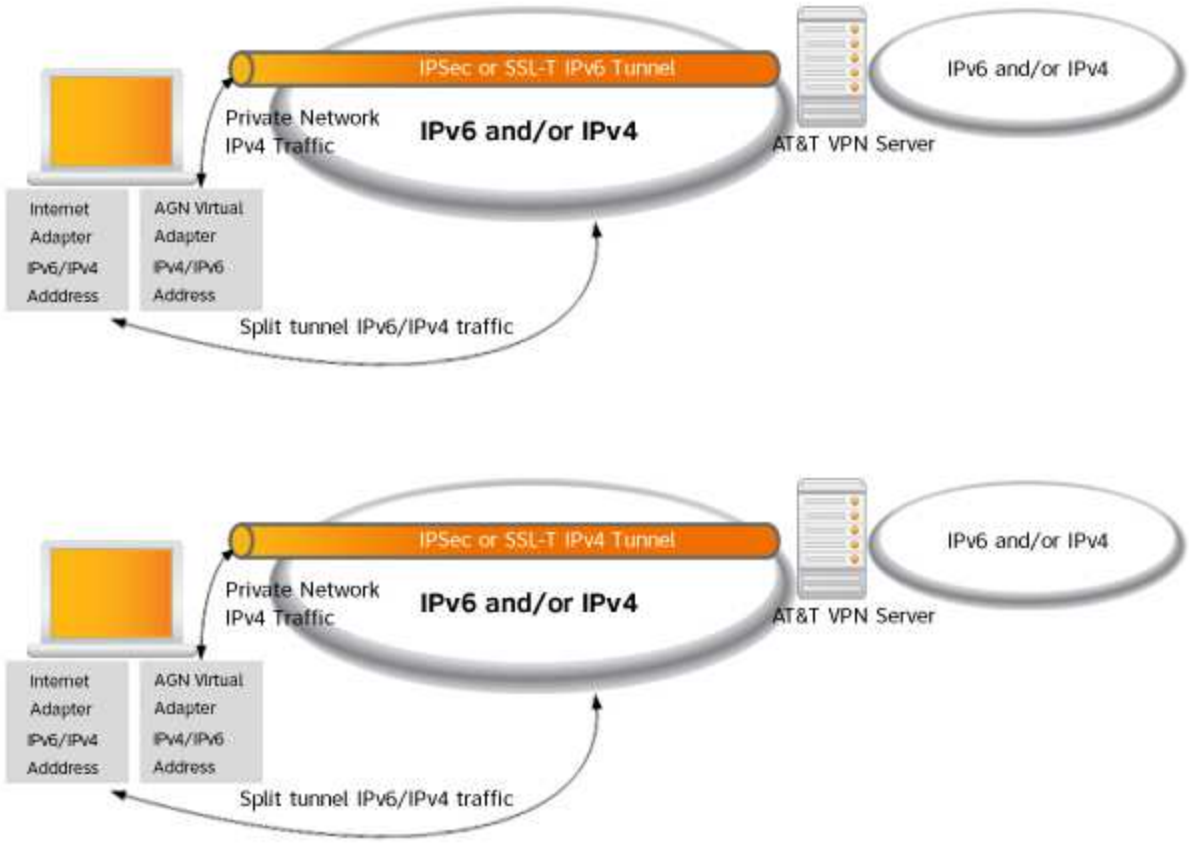


Figure 46: IPv6 Support

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

IP version preference

The AT&T Global Network Client can be configured to prefer an IP version for establishing a VPN connection when connected to an IPv4/IPv6 dual stacked network. The default preference is currently IPv4. This setting is centrally configured through the AT&T administration server.

IP version failover

Granular control over the number of VPN connection attempts to make with the preferred IP version is supported. This setting is only pertinent on IPv4/IPv6 dual stack networks. The default number of VPN connection attempts per IP version is defaulted to 2. This setting is centrally configured through the AT&T administration server.

For example, if there are 3 VPN servers and IPv6 is preferred. The AT&T Global Network Client's connection attempt list would be ordered as follows:

1. Attempt VPN server 1 using IPv6.
2. Attempt VPN server 2 using IPv6.
3. Attempt VPN server 1 using IPv4.
4. Attempt VPN server 3 using IPv6.
5. Attempt VPN server 2 using IPv4.
6. Attempt VPN server 3 using IPv4.

OPSWAT Certified VPN

The AT&T Global Network Client VPN is certified through the OPSWAT Certification Program. This certification demonstrates that the AT&T Global Network Client VPN is compatible with products from other market-leading technology vendors. Products carrying OPSWAT certification follow standards that indicate they will not adversely affect other installed security software. To learn more, visit the OPSWAT Certification website at http://www.opswat.com/certified.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Integrating with Third Party Software

Although the AT&T Global Network Client contains an integrated VPN client that supports multiple tunnel endpoints, some customers prefer to use a third-party VPN client and use the AT&T Global Network Client to establish an underlying Internet connection. Examples of third party software VPN clients that the AT&T Global Network Client integrates well with are Cisco AnyConnect®[8] and NetMotion®[9] Mobility XE®.

In other cases, the AT&T Global Network Client is used to establish the VPN connection and third party software is used as the underlying Internet connection. This section describes how the AT&T Global Network Client interacts with some third party software clients.

Changes in the NetMotion client status are logged to the message log.

ThinkVantage® Access Connections™[10]

ThinkVantage® Access Connections™ is a connectivity assistant program for your ThinkPad computer. When a Wi-Fi or mobile connection is made, there can be contention between the ThinkVantage Access Connections client and the AT&T Global Network Client.

The user can specify which software client is in control of the connection by clicking on **Login Properties**, **Preferences** tab, and checking the box next to **Disable Lenovo Access Connections** under the **When this program starts** section. This checkbox is only visible when the Access Connections software is detected on the user's computer.

If this checkbox is checked (default), the AT&T Global Network Client will assume control of both Wi-Fi and mobile access on startup and will disable the Access Connections software if running. If the AT&T Global Network Client does disable Access Connections on start up, it will re-enable it before exiting.

If this checkbox is *not* checked, the AT&T Global Network Client will disable its own Wi-Fi and mobile control and allow Access Connections to control the network access.

WireShark® and Microsoft Network Monitor

Network traffic analysis tools, WireShark®[11] and Microsoft Network Monitor are supported with AT&T Global Network Client 9.1 and later. The network traffic will be logged to the dynamic VPN IP address of the AT&T Global Network Client VPN session being monitored. The MAC address of the VPN adapter is statically defined in the AT&T Global Network Client and will be the same across all instances of the AT&T Global Network Client on the network, the IP address must be used to identify individual machine activity.

[8] Cisco AnyConnect® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.
[9] NetMotion® is a registered trademark, and NetMotion Wireless Locality™, Mobility XE®, Roamable IPSec™, InterNetwork Roaming™, Best-Bandwidth Routing™, and Analytics Module™ are trademarks of NetMotion Wireless, Inc.
[10] ThinkVanatage® and Access Connections™ are trademarks of Lenovo in the United States, other countries, or both.
[11] Wireshark and the "fin" logo are registered trademarks of the Wireshark Foundation

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Help/Customer Support

Support Forum

AT&T offers an on-line support forum for topics related to the AT&T Global Network Client. Access the forum via your web browser at:

http://bizcommunity.att.com

You must register as a user to access all features of the support forum. You can post questions for AT&T development and support personnel as well as access support documents and presentations via the forum.

Contact AT&T

In the **Help** panel on the main window, click **Contact customer support** to open the **Customer Support** window containing your AT&T help desk phone numbers.

Figure 47: Customer Support Window

In addition to calling for support you can click **View support log…** to open a web page with useful information about your installation of the AT&T Client.

Click **Close** to return to the AT&T Client.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Frequently Asked Administration Topics

Using Digital Certificates for Authentication

AT&T offers the use of x.509v3 Entrust and Microsoft digital certificates to authenticate users for Internet and Managed VPN services.

AT&T does not create, distribute or maintain user digital certificates. You must support your own digital certificate infrastructure. AT&T uses the common name as the user ID / unique identifier; therefore you must enforce uniqueness on this attribute. The AT&T Custom Development Team can work with you to use a limited list of other attributes as well. Contact your AT&T account team for further assistance with Digital Certificate Authentication.

When using Digital Certificates for authentication you must use Public Properties to set them correctly for use. See the Customizations Chapter on page 48 of this guide for additional information about Public Properties.

Additionally, the use of Digital Certificates must be configured centrally in the AT&T administration server.

If your company is using more than one certificate, the user will be prompted to select which signature certificate to use for their connection (encrypted certificates are not displayed).

Using Mobile Monitoring Programs

When connecting with the AT&T Global Network Client using a Mobile service, the AT&T Global Network Client may interfere with third party programs that monitor your mobile connectivity (usually supplied by your Mobile Provider). Click **Login Properties**, **Preferences** tab, check the box next to **Permanently disable cellular device support** to disable the AT&T Global Network Client monitoring of your mobile activity and allow the third party program access to the mobile data. To enable monitoring, uncheck the box next to **Permanently disable cellular device support**. You must restart the AT&T Global Network Client for monitoring to resume.

Connecting Directly to a Mobile or Wi-Fi Network

Installation Option for Mobile Internet Connections

Some networks do not require AT&T Global Network authentication to obtain network access. There are two options that will allow users to connect directly to mobile or Wi-Fi networks without entering AT&T Global Network credentials. During install a user can select the Custom Installation and check the "Default to "Internet" for network connections that do not require RAS credentials" checkbox under **Network Access Options**. This checkbox is tied to the **INTERNET_ONLY** Windows Installer public property and will not require RAS credentials for mobile or Wi-Fi use. Alternately, an administrator can set this checkbox to default to being selected for all users at install time by referring to the INTERNET_ONLY public property in the Customizations section of this document.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

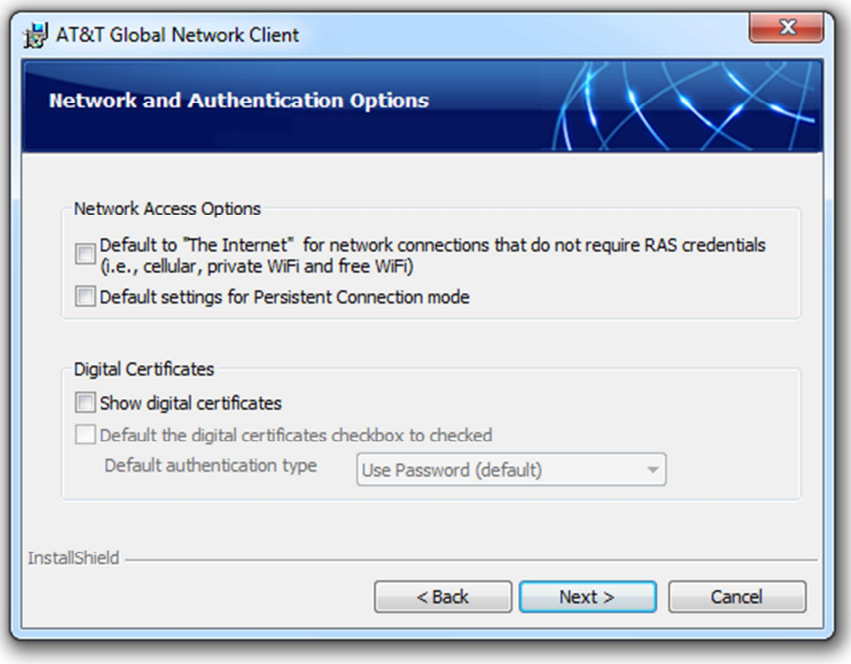

AT&T Global Network Client
Network and Authentication Options
Network Access Options
Default to "The Internet" for network connections that do not require RAS credentials (i.e., cellular, private WiFi and free WiFi)
Default settings for Persistent Connection mode
Digital Certificates
Show digital certificates
Default the digital certificates checkbox to checked
Default authentication type
Use Password (default)
InstallShield
< Back
Next >
Cancel

Figure 48: Network Access Options

Troubleshooting Installation

The AT&T Global Network Client *executable* (not MSI file) installation package automatically generates an installation log file and places it in the %temp% folder. The log file name will mimic the installation file name, with .log replacing the installation file extension.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Appendix A: Central Configuration

The AT&T administration server stores the configuration information for all users, including service type and service options. The AT&T Global Network Client interfaces with the AT&T administration server to retrieve values set by you, the Customer Account Administrator. The AT&T administration server supports a tiered architecture. You can set values at three levels: Model, Account, or UserID. Models are thr highest level and can apply to multiple accounts. Accounts are the second level and typically have many userids assigned to an account. User IDs are the lowest level and typically are assigned to a single end user.

Configuration of the values can be done by your AT&T representative or by you, via an AT&T provided administration tool, AT&T Global Network Services Customer Support Tools and Reports, located at http://globalnetwork.support.att.com. Click the link for **Encrypted access to web tools and reports** under the AT&T Managed Network Services (MNS) Tools/Reports section located on the main page. Enter your **Account**, **User ID** and **Password** to login. After login select **Administration Tools for AT&T Service Manager** from the drop down list on the top of the screen. Click **Guide** on the **Navigation Menu** on the left hand side of the screen to access the "Administration Tools for AT&T Service Manager Guide". All AT&T Accounts/User IDs are not authorized to use the tools; and access requires configuration by AT&T. Contact your AT&T representative for additional assistance using AT&T Global Network Services Customer Support Tools and Reports.

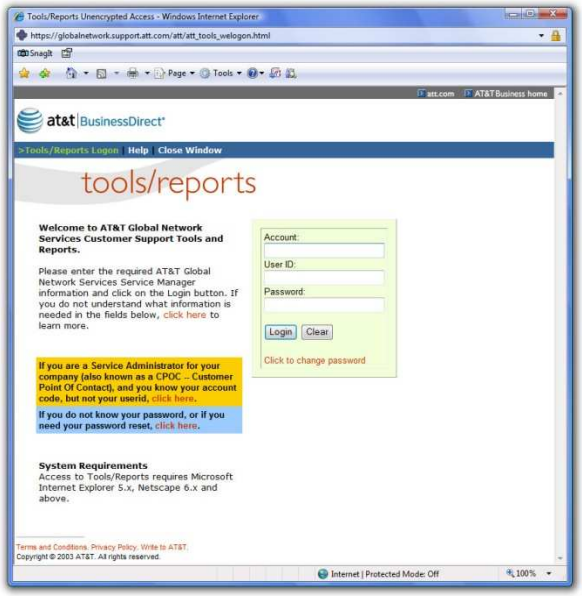

Tools/Reports Unencrypted Access - Windows Internet Explorer
https://globalnetwork.support.att.com/att/att_tools_welogon.html
at&t BusinessDirect
>Tools/Reports Logon | Help | Close Window
tools/reports
Welcome to AT&T Global Network Services Customer Support Tools and Reports.
Please enter the required AT&T Global Network Services Service Manager information and click on the Login button. If you do not understand what information is needed in the fields below, click here to learn more.
Account:
User ID:
Password:
Login
Clear
Click to change password
If you are a Service Administrator for your company (also known as a CPOC -- Customer Point Of Contact), and you know your account code, but not your userid, click here.
If you do not know your password, or if you need your password reset, click here.
System Requirements
Access to Tools/Reports requires Microsoft Internet Explorer 5.x, Netscape 6.x and above.
Terms and Conditions. Privacy Policy. Write to AT&T.
Copyright © 2003 AT&T. All rights reserved.
Internet | Protected Mode: Off
100%

Figure 49: AT&T Administration Server Configuration Tool

The AT&T Global Network Client configuration values in the AT&T administration server are shown in the table in the next section. Inaccurate configuration of central values can produce unexpected results and errors for your users, questions about any of the individual fields should be directed to your AT&T account representative prior to making changes.

Central Configuration Values

Retrieval of Network Settings Over an Existing Internet Connection

For Internet over broadband connections the AT&T Global Network Client will query the user to retrieve the network settings. After connecting, if a profile containing an account and user id is active, the default service will be "Internet" and the connection will take place over an existing Internet connection.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

The AT&T Global Network Client will retrieve the following fields from the Service Manager and save to the user profile:

- Default Service
- Wi-Fi bitmask
- Custom program updates info (ftp server and ftp path)

AT&T Administration Server Client Configuration Values

Field	Info	Default	Value/Behavior
General Service Options			
Activity Threshold Timeout	Optional Will inherit from model	Blank	Set to number in range: 1-60 Specifies a numeric value in minutes which defines the maximum time which can transpire before the AT&T Global Network Client will timeout the user.
Activity threshold Bytes	Optional Will inherit from model	Blank	Set to number in range: 50-50,000 Specifies a numeric value in bytes defining the minimum size of an IP packet which would indicate user activity (minimizes chatty applications such as IM retaining a connection after actual user activity has stopped)
Authentication Method	Required	R	D – Radius L – LDAP R – RACF S – SecurID W – SafeWord

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Field	Info	Default	Value/Behavior
Default Service Type[12]	Required		03 = LAN Dial 06 = Internet 07 = Async Terminal Services (ATS) 08 = Async Pass Through 0A = VPEF (VCOM, XPC) 0B = Multi-Protocol Tunneling (MPT, LAN Dial V2) 0C = Fixed IP 0D = Managed Tunneling Service using PPTP (MTS/PPTP 0E = Managed Tunneling Service using PPTP with Multi-Protocol 0F = TCP Clear 10 = Managed Tunneling Service using IPSec (MTS/IPSec) 11 = 3D (Internet, Common Services, Tunneling) 12 = Managed Tunneling Services using IPSec with Dual Access
DNS	Recommended	Blank	Specifies Primary & Secondary DNS for your account Beginning with Version 8.0, setting this value to Blank will remove any previously cached customized value from the AT&T Global Network Client.

[12] See Additional Service Information Section of this guide for descriptions.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Field	Info	Default	Value/Behavior
Domain Name	Recommended	Blank	The domain name to be active for the session. Beginning with Version 8.0, setting this value to Blank will remove any previously cached customized value from the AT&T Global Network Client.
Domain Search Suffix 1-5 –	Optional	Blank	Up to 5 domain suffixes may be entered to aid in web address searching (for example, att.com). Beginning with Version 8.0, setting this value to Blank will remove any previously cached customized value from the AT&T Global Network Client.
Help Desk Number	Optional	Blank	xxx-xxx-xxxx - Defines the Help Desk Phone number that will appear in the AT&T Global Network Client
Local Subnet Access	Allows users that are not configured for Dual Access or split tunneling to access resources on their directly connected subnet	N	Y = Allow local subnet access N = Do not allow local subnet access

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Field	Info	Default	Value/Behavior
Network Awareness	Optional	N	When set the AT&T Global Network Client will use values in the NetworkAwareness.xml file to define actions for networks. (see Network Awareness Customization) Y=Enable Network Awareness and use values in xml file N=Disable Network Awareness, ignore xml file.
Persistent Connection	Optional	Y	Enables the Persistent Connection feature Y=Allow Persistent Connections N=Do Not Allow Persistent Connections
Save Password Expiration Interval	Optional	0	Defines the number of hours after which a user is forced to reenter their password, even if the "Save Password" option is enabled in the AT&T Client. 0=Never #=Number of hours until the user is forced to enter their password
Time For Password to Expire			Can only be updated by AT&T. support personnel
VPN Mobility	Optional	N	Specifies if the VPN Mobility feature is enabled. Y=Enabled N=Disabled

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Field	Info	Default	Value/Behavior
VPN Mobility Duration	Optional	600	Amount of time in seconds for which a VPN Server will hold VPN Session information after losing connectivity with the AT&T Global Network Client to allow VPN Mobility the ability to reestablish the same session. 0=None 1-9999=Number of seconds. *Setting this to a large value may impact server performance
WINS	Recommended	Blank	Specifies the primary and secondary WINS values for your account.
Dial/ISDN Service Options			
Analog Auto Dial Backup	Optional	Blank	0 = Automatic Backup is not allowed 1 = Automatic Backup is allowed using 1 line 2 = Automatic Backup is allowed using 2 bundled lines U = Automatic Backup is allowed using an unlimited number of bundled lines
Dial Session Timeout	Optional		Specifies the time, in minutes, that the Dial Session will maintain a connection before a timeout occurs and the session is dropped. Valid range is 1 through 7,200.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Field	Info	Default	Value/Behavior
Extended Access Allowed	Optional	Blank	Y = user is allowed Extended Access N = user is not allowed Extended Access
Idle Dial Timeout	Optional	Blank (the value is determined by the dial gateway)	Set to number in range: 1 - 720 for all services except Internet Set to number in range: 1 – 35 for Internet service 999 to specify no Idle Dial Timeout. (not permitted for Internet service)
ISDN auto backup	Optional	Blank	0 = ISDN Automatic Backup is not allowed 1 = ISDN Automatic Backup is allowed using 1 B channel 2 = ISDN Automatic Backup is allowed using 2 bonded B channels U = ISDN Automatic Backup is allowed using an unlimited number of bundled lines
AT&T Global Network Client Firewall			
Enable AT&T Global Network Client Firewall	Optional Will inherit from Model	Blank	Y – AT&T Global Network Client Firewall is enabled N – AT&T Global Network Client Firewall is disabled
User Controlled Firewall	Optional Will inherit from Model	Blank	Y – User has modify access to Firewall Settings Window. N – User can not modify settings on Firewall Settings Window.
AT&T VPN			

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Field	Info	Default	Value/Behavior
AT&T Global Network Client IPSec Failover	Optional	Blank	Y– Dynamically failover to Transparent Tunneling (SSL-T) service if the IPSec connection fails for any reason. N – Do not failover to Transparent Tunneling
Allow Access List Exceptions	Optional	Blank/N	Y = Allow users to define exceptions to VPN access list N = Do not allow users to define exceptions to VPN access list
Allow User Switches[13]	Optional	Blank	Y = Allow computer to remain VPN connected under current Windows user account when performing Fast User Switch (client remains running) or User Logoff (client will exit but connection persists) on local PC. N = Exits client and terminates VPN session when performing Fast User Switch or User Logoff on local PC.

[13] Keeping a VPN connection active after a Fast User Switch or User Logoff can produce unexpected results and is a potential security risk; therefore it is recommended this value only be set to Y for short term troubleshooting purposes.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Field	Info	Default	Value/Behavior
IPSec VPN Tunnel Settings			Set Encryption to: DES Triple DES AES 128 AES 192 AES 256 Set Authentication to: HMAC – SHA1 HMAC – MD5 Set Compression: LZS
Negotiate UDP	Optional	Blank	Y = Negotiate UDP Encapsulation N = Do not negotiate

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Field	Info	Default	Value/Behavior
SSL AT&T Global Network Client Allow Proxy –	This option only works on AT&T VPN Servers (SIG/GIG - MTS-IPSec and MTS-IPSec DA) connections. You must profile your users for AT&T VPN Tunneling Services SSL, AT&T VPN Tunneling Services IPSec, and Transparent Tunneling (SSL-T).		Y = Dynamically failover to SSL-T service if a proxy is detected. N = Do not dynamically failover to SSL-T if a proxy is detected.
Tunnel Dual Access	Optional	Blank	Y = Managed Tunneling Service Dual Access is enabled and the user is allowed to access Internet locations. N = Managed Tunneling Service Dual Access is disabled and the user can not access Internet locations.

Figure 50: Central Configuration Values Table

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Additional Service Information

Business Internet Service

An Internet dial service, which gives you multiple email accounts and access to news groups.

FixedIP

The FixedIP service provides remote access to your company's private Intranet via a network-based VPN to a VPN server on your Intranet. The assigned IP address can be static or assigned from a customer-specific address pool on your VPN server. The service supports multiple protocols and provides centrally managed network-based subnet filtering and network-based firewall security. This is a network based VPN service and no VPN software is required on the workstation.

FixedIP DualAccess

The FixedIP DualAccess service is the same as the FixedIP service with the addition of being able to access to the Internet using the same network connection.

Managed IPSec VPN

Managed IPSec VPN provides remote access to a company's private network via an end to end IPSec VPN from the AT&T Global Network Client to a VPN server (AT&T SIG or Cisco) on your company's private Intranet. The service provides centrally managed subnet filtering on the workstation and local firewall security as well as centrally managed network-based subnet filtering and network-based firewall security.

Managed IPSec DualAccess VPN

The Managed IPSec DualAccess VPN is the same as Managed IPSec VPN with the addition of being able to access the Internet using the same network connection.

Managed IPSec Authentication Method

The authentication for the VPN is provided by the AT&T Global Network authentication server. The authentication can be performed directly by the Central Authentication Server or the Central Authentication Server can proxy to/verify the request with a customer managed authentication server.

Managed SSL VPN

The SSL VPN service, also known as Transparent Tunneling, traverses customer site proxies and firewalls using SSL to minimize network configuration changes normally required for IPSec VPN tunneling. SSL VPN is useful for connecting from locations that block IPSec or only allow Internet access through a proxy server. AT&T SSL VPN is terminated by an AT&T SIG VPN Server.

Managed SSL Dual Access VPN

The Managed VPN SSL DualAccess VPN is the same as SSL VPN with the addition of being able to access the Internet using the same network connection

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Appendix B: Supported Mobile Devices

AT&T Supported Mobile Devices

Device drivers for the following list of devices are available for installation with the Managed VPN Edition of the AT&T Global Network Client.

Modem Cards	Minimum Version	Last Client Release Supported
AT&T USBConnect Beam	9.2	
AT&T Sierra Wireless AC890 (AC504, Triple Lindy)	8.0.3	9.3.2
AT&T USBConnect 881 Card	7.2.0	8.8.0
AT&T USBConnect Elevate 4G	8.7.0	9.3.2
AT&T USBConnect Force 4G	8.7.0	9.3.2
AT&T USBConnect Lightning	8.1.0	9.3.2
AT&T USBConnect Momentum 4G	9.1	
AT&T USBConnect Turbo	8.0.3	9.3.2
AT&T USBConnect Velocity	8.0.3	9.3.2
AT&T USBConnect Shockwave	8.3.2	
AT&T USBConnect Adrenaline	8.4.0	9.3.2
AT&T USBConnect 900 (E1815)	8.6.0	9.3.2
Sierra Wireless AirCard 890	8.4.0	
Huawei Force 4G (E368)	8.6.0	9.3.2
Novatel U730 Card (Windows XP SP2+)	7.2.0	8.8.0
Option Globetrotter Combo Card (Windows XP only)	7.2.0	8.8.0
Option GT MAX 1.8 Card	7.2.0	8.8.0
Option GT Max 3.6 Card	7.2.0	8.8.0
Option GT Max 3.6 Express Card	7.2.0	8.8.0
Option GT Ultra Card	7.2.0	8.8.0

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Modem Cards	Minimum Version	Last Client Release Supported
Option GT Ultra Express Card	7.2.0	8.8.0
Option *i*Con 3.6U5i (322 / Faema / AT&T Quicksilver)	7.5.0	8.8.0
Sierra Wireless AirCard 750 Card	7.2.0	8.8.0
Sierra Wireless AirCard 775 Card	7.2.0	8.8.0
Sierra Wireless AirCard 860 Card	7.2.0	8.6.0
Sierra Wireless AirCard 875 Card	7.2.0	8.6.0
Sierra Wireless AirCard 875U Card	7.2.0	8.6.0
Sierra Wireless AirCard 881 Card	7.2.0	8.9.1
Sierra Wireless USBConnect Mercury (Poptart)	7.5.0	8.9.1
Sony Ericsson GC82 Card	7.2.0	8.9.1
Sony Ericsson GC83 Card	7.2.0	8.9.1
Sony Ericsson W518a	8.0.2	9.3.2

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

NETBOOKS	Minimum Version	SDK Used in latest Release	Last Client Release Supported
Acer Aspire One	8.0.2	GOBI 1000	
HP Iverson	8.0.2		
Lenovo S10	8.0.2		
Samsung Go (Pebble)	8.0.2		
Nokia Booklet 3G	8.0.2	WMB 7.0	
Dell 11z	8.0.2		
HP MINI 5102	8.0.2	GOBI 2000	
HP Mini 110-3000	8.0.2	WMB 7.0	

* WMB = Windows Mobile Broadband

Compatible Phones[14]	Minimum Version	Last Client Release Supported
AT&T Quickfire	7.6.1	8.9.1
AT&T Tilt	7.2.0	8.9.1
HP iPAQ Obsidian	8.0.2	9.3.2
HTC FUZE	7.6.1	8.9.1
LG Arena (GT950)	8.0.2	9.3.2
LG CB630	7.6.0	8.9.1
LG CF360	7.6.1	8.9.1
LG Chiwoo CU515	7.6.0	8.9.1
LG CU320	7.2.0	8.9.1
LG CU400	7.2.0	8.9.1
LG CU500	7.2.0	8.9.1
LG INCITE	7.6.1	8.9.1

[14] If using your handset as a tethered modem, you may need a data cable accessory, sold separately, to connect the phone to your PC.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Compatible Phones[14]	Minimum Version	Last Client Release Supported
LG Invision	7.6.1	8.9.1
LG Monaco (GW820)	8.0.2	9.3.2
LG Secret	7.6.1	8.9.1
LG Shine II (GD710)	8.0.2	9.3.2
LG TRAX	7.2.0	8.9.1
Motorola Tundra	7.6.1	8.9.1
Motorola V180	7.2.0	8.9.1
Motorola V220	7.2.0	8.9.1
Motorola V400	7.2.0	8.9.1
Motorola V551	7.2.0	8.9.1
Motorola V3xx	7.2.0	8.9.1
Motorola RAZR V3	7.2.0	8.9.1
Motorola Z9 "Husky"	7.5.0	8.9.1
Nokia 6350	8.0.2	9.3.2
Nokia 6650	7.6.1	8.9.1
Nokia Mural (6750)	8.0.2	9.3.2
Nokia Surge (6790)	8.0.2	9.3.2
Pantech C530	7.6.1	8.9.1
Pantech C610	7.6.1	8.9.1
Pantech C630	7.6.1	8.9.1
Pantech Duo Pro	7.6.1	8.9.1
Pantech Matrix	7.6.1	8.9.1
Research In Motion BlackBerry 8700c	7.2.0	8.9.1
Research In Motion BlackBerry 8800	7.2.0	8.9.1
Research In Motion BlackBerry 8820	7.2.0	8.9.1
Research In Motion BlackBerry 8110	7.5.0	8.9.1
Research In Motion BlackBerry Bold 9700	8.0.2	9.3.2

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Compatible Phones[14]	Minimum Version	Last Client Release Supported
Research In Motion BlackBerry Bold 9800	8.1.2	9.3.2
Research In Motion BlackBerry Bold 9900	9.1	
Research In Motion BlackBerry Curve 8300	7.2.0	8.9.1
Research In Motion BlackBerry Curve 8310	7.2.0	8.9.1
Research In Motion BlackBerry Curve 8320	7.5.0	8.9.1
Research In Motion BlackBerry Curve 9300	9.1	
Research In Motion BlackBerry Curve 9360	9.1	
Research In Motion BlackBerry Curve 9860	9.1	
Research In Motion BlackBerry 9000 Raptor / Bold	7.5.0	8.9.1
Research In Motion BlackBerry Gemini 8520	8.0.2	9.3.2
Research In Motion BlackBerry Pearl	7.2.0	8.9.1
Research In Motion BlackBerry Torch 9800	8.10.0	
Samsung A707 Sync	7.2.0	8.9.1
Samsung A717	7.2.0	8.9.1
Samsung A727	7.2.0	8.9.1
Samsung A777	7.6.1	8.9.1
Samsung A797	8.0.2	9.3.2
Samsung A887	8.0.2	9.3.2
Samsung A897	8.0.2	9.3.2
Samsung BJ Plus i617	7.3.0	8.9.1
Samsung Eternity	7.6.1	8.9.1
Samsung i607 Blackjack	7.2.0	8.9.1
Samsung i907 Mirage	7.5.0	8.9.1
Samsung Peridot SGH A737	7.3.0	8.9.1
Samsung Propel	7.6.1	8.9.1
Samsung Rugby SGH-A837	7.5.0	8.9.1
Samsung ZX10	7.2.0	8.9.1

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Compatible Phones[14]	Minimum Version	Last Client Release Supported
Samsung ZX20	7.2.0	8.9.1
Sony Ericsson W760a	7.6.1	8.9.1
Sony Ericsson Bear Z750a	7.5.0	8.9.1

Mobility SDK Technology Use

SDK used on Windows 7 and Windows 8 with Mobility Broadband Technologies.

DEVICE	CDMA				GSM	
	USING NDIS		USING RAS			
	USING WMB	NOT USING WMB	USING WMB	NOT USING WMB	USING WMB	NOT USING WMB
Sierra						
Most Devices	WMB SDK	Sierra CDMA SDK	Sierra CDMA SDK	Sierra CDMA SDK	Sierra GSM SDK	Sierra GSM SDK
Lightning with older Firmware	N/A	N/A	N/A	N/A	N/A	AT Command SDK
GOBI 1000	GOBI SDK	Not Tested	GOBI SDK	Not Tested	GOBI SDK	Not Tested
GOBI 2000	GOBI SDK	Not Tested	GOBI SDK	Not Tested	GOBI SDK	Not Tested
GOBI 3000	Sierra GOBI SDK	Not Tested	Sierra GOBI SDK	Not Tested	Sierra GOBI SDK	Not Tested
Huawei						
Silk E1815	N/A	N/A	N/A	N/A	WMB SDK	Smartcom SDK
Force 4G	N/A	N/A	N/A	N/A	WMB SDK	Smartcom SDK
LG						
Adrenaline	N/A	N/A	N/A	N/A	WMB SDK	Smartcom SDK
Option						
Most Devices	WMB	Not	AT Comman	AT Command	WMB SDK	Option SDK

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	CDMA				GSM	
	USING NDIS		USING RAS			
	USING WMB	NOT USING WMB	USING WMB	NOT USING WMB	USING WMB	NOT USING WMB
	SDK	Detected	d SDK	SDK		
Other Devices						
Most Devices	WMB SDK	Not Detected	AT Command SDK	AT Command SDK	WMB SDK	AT Command SDK

Embedded Modules

The following list of embedded modules tested.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[15]	AT&T CLIENT MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
Alcatel					
X220l	USB	GSM	Supported	8.2	

Other Supported Mobile Devices

The following list of devices is supported for use with the AT&T Client, but installation and configuration of the device must be manually performed outside of the AT&T Global Network Client installation process.

[15] SDK Definitions:

Supported: Device has been tested by Smith Micro (provider of the SDK) against a version of the SDK.

Certified: Device has specifically been tested by AT&T against the version of the AT&T Global Network client listed.

Pending: Device is pending certification by AT&T.

Not Supported: Device is either not tested or does not work.

* Devices marked by an asterisk are known by more than one name.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
Alcatel					
X220l	USB	GSM	Supported	8.2	
Asus					
Halley	Handset	HSDPA	Supported	7.0	8.9.1
Bandrich					
M250	Embedded	HSDPA	Supported	8.0.2	8.10
M280	Embedded	HSDPA	Certified	8.0.2	8.10
Dell					
Dell 5540 Mobile Broadband	Embedded	HSUPA	Certified	8.0.2	8.10
Dell 5505 Mobile Broadband	Embedded	HSDPA	Supported	6.9	8.9.1
Dell 5510 Mobile Broadband	ExpressCard/ Embedded	HSDPA 3.6	Supported	6.9	8.9.1
Dell 5520 Mobile Broadband	Embedded	HSDPA 3.6	Supported	7.3	8.9.1
Dell 5530 Mobile Broadband	Embedded	HSUPA	Supported	7.3	8.9.1
Dell 5720 Mobile Broadband	Embedded	EVDO	Supported	7.4	8.9.1
Dell 5600 Mobile Broadband	Embedded	EVDO/HSPA	Certified	8.0.3	8.10
Dell 5620 Mobile Broadband	Embedded	EVDO/HSPA	Certified	8.0.2	8.10

[16] SDK Definitions:

Supported: Device has been tested by Smith Micro (provider of the SDK) against a version of the SDK.

Certified: Device has specifically been tested by AT&T against the version of the AT&T Global Network client listed.

Pending: Device is pending certification by AT&T.

Not Supported: Device is either not tested or does not work.

* Devices marked by an asterisk are known by more than one name.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
Ericsson					
R520m	Handset	GPRS	Supported	6.7	8.9.1
F3307	Embedded	HSUPA	Certified	8.0.2	8.10
F3507g	Embedded	HSUPA	Certified	7.3	8.9.1
F3607gw	Embedded	HSUPA	Pending	8.0.2	8.10
F5521gw	Embedded	HSUPA	Pending	8.2	9.3.2
Franklin Wireless					
CDU680	USB	EVDO	Supported	8.0.2	8.10
CMU300	USB	EVDO	Supported	8.0.2	8.10
CMU301	USB	EVDO	Supported	8.1.1	9.3.2
U600 (Dual Mode Device)	USB	EVDO	Supported	8.3.2	9.3.2
M600 (Dual Mode Device)	Embedded	EVDO	Supported	8.3.2	9.3.2
Fujistu					
F2402*	PC Card	WCDMA	Supported	6.7	8.9.1
P2402	PC Card	WCDMA	Supported	6.7	8.9.1
MC8781*	Embedded	HSUPA	Supported	7.3	8.9.1
HP					8.9.1
HS2300*	USB	HSDPA	Supported	7.2	8.9.1
HS2600(?)*	Embedded	HSUPA	Pending	7.3	8.9.1
un2400*	Embedded	HSUPA	Certified	7.3	8.9.1
un2420*	Embedded	HSUPA	Pending	8.0.2	8.10
QC430AA	Embedded	HSUPA/EVDO	Supported	8.8	
QC430UT	Embedded	HSUPA/EVDO	Supported	8.8	
HTC					
4600/4605	Handset	GSM	Supported	8.0.2	8.10
8900/8925	Handset	GSM	Supported	8.0.2	8.10
Huawei					
E169	USB	HSDPA	Supported	7.3	8.9.1

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
E17X (E170/E172)	USB	HSDPA	Supported	7.3	8.9.1
E220	USB	HSDPA	Supported	6.9	8.9.1
E226	USB	HSDPA	Supported	8.0.2	8.10
EC228	USB	EVDO	Supported	8.0.2	8.10
E230	USB	HSDPA	Supported	7.4	8.9.1
E270	USB	HSDPA	Supported	7.1	8.9.1
E272*	USB	HSDPA	Supported	7.2	8.9.1
E280	USB	HSDPA	Supported	7.1	8.9.1
EC360	USB	EVDO	Supported	8.0.2	8.10
E510	PC Card	UMTS	Certified	7.4	8.9.1
E600	PC Card	UMTS	Supported	6.7	8.9.1
E612	PC Card	UMTS	Supported	7.4	8.9.1
E618	PC Card	UMTS	Supported	6.7	8.9.1
E620	PC Card	HSDPA	Supported	6.7	8.9.1
E621	PC Card	HSDPA	Supported	6.7	8.9.1
E630	PC Card	HSDPA	Supported	6.9	8.9.1
E660A	PC Card	HSDPA 7.2	Supported	6.9	8.9.1
EM730	Embedded	HSDPA 7.2	Supported	8.0.2	8.10
E770	Embedded	HSDPA 7.2	Supported	8.0.2	8.10
EM770w	Embedded	HSDPA 7.2	Certified	8.0.2	8.10
E800	PC Card	HSDPA 7.2	Supported	7.1	8.9.1
E800A	PC Card	HSDPA 7.2	Supported	7.1	8.9.1
E870	PC Card	HSDPA 7.2	Supported	7.1	8.9.1
B970	USB	EDGE	Supported	8.0.2	8.10
E3565 (E160G)	PC Card	GPRS/EDGE	Certified	7.4	8.10
E3735 (E880)	PC Card	GPRS/EDGE	Certified	7.4	8.10
K3715 (E180, E182)	USB	HSDPA	Certified	7.4	8.9.1
EG162	PC Card	GPRS/EDGE	Supported	7.3	8.9.1

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
K3520	USB	HSDPA	Supported	8.0.2	8.10
M3710	USB	HSDPA	Supported	8.0.2	8.10
K3565	USB	HSDPA	Supported	8.0.2	8.10
E1762v	PC Card	HSDPA	Certified	8.0.2	8.10
E1615	PC Card	HSDPA	Supported	8.0.2	8.10
E1550	USB	HSDPA	Supported	8.0.2	8.10
E1552	USB	HSDPA	Supported	8.0.2	8.10
K3765	USB	HSDPA	Supported	8.0.2	8.10
K4505	USB	HSDPA	Supported	8.0.2	8.10
UMG181	USB	HSDPA	Supported	8.1	8.10
UMG1691	USB	HSDPA	Supported	8.1	8.10
E168 (EC168)	USB	HSDPA	Supported	8.1	8.10
E1820	USB	HSDPA	Supported	8.1	8.10
E1756	USB	HSDPA	Supported	8.1	8.10
R201	USB	HSDPA	Supported	8.2	8.10
K4605	USB	HSPA	Supported	8.3.2	8.10
K3806	USB	HSPA	Supported	8.3.2	8.10
E820	Embedded	HSDPA 7.2	Supported	8.3.2	8.10
Imate					
Jas Jam	Handset	GPRS	Supported	6.9	8.9.1
SP Jas	Handset	GPRS	Supported	6.9	8.9.1
Kyocera					
KPC650	PC Card	1xEVDO/1xRTT	Supported	6.7	8.9.1
KPC680	Express Card	1xEVDO	Supported	8.0.2	8.10
Lenovo					
MC8775*	Embedded	HSDPA	Supported	7.1	8.9.1
LG					
A7110	Handset	EDGE	Supported	6.7	8.9.1
C1300	Handset	GPRS	Supported	6.7	8.9.1

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
G4050	Handset	GPRS	Supported	6.7	8.9.1
L1200	Handset	GPRS	Supported	6.7	8.9.1
L1400	Handset	GPRS	Supported	6.7	8.9.1
LX160	Handset	EVDO	Supported	7.3	8.9.1
LX400	Handset	EVDO	Supported	7.3	8.9.1
LX550	Handset	EVDO	Supported	7.3	8.9.1
LX570	Handset	EVDO	Supported	7.3	8.9.1
LX600	Handset	EVDO	Supported	8.0.2	8.10
AX840	Handset	EVDO	Supported	8.2	8.10
CU320	Handset	UMTS	Supported	6.7	8.9.1
CB630	Handset	UMTS	Supported	8.0.2	8.10
CU500	Handset	UMTS	Supported	6.7	8.9.1
CU515*	Handset	HSDPA	Supported	7.3	8.9.1
CU720	Handset	UMTS	Supported	7.3	8.9.1
CU920	Handset	HSDPA	Supported	7.3	8.9.1
CU575*	Handset	UMTS	Supported	7.1	8.9.1
X110	Embedded	HSUPA	Supported	8.0.2	8.10
GR500	Handset	HSUPA	Supported	8.0.2	8.10
Bobsleigh	USB	HSUPA	Supported	8.0.2	8.10
GT950	Handset	HSUPA	Supported	8.0.2	8.10
GW820	Handset	HSUPA	Supported	8.0.2	8.10
GD710	Handset	HSUPA	Supported	8.0.2	8.10
GR700	Handset	HSUPA	Supported	8.1	8.10
AC8370	Handset	EVDO	Supported	8.3.2	8.10
Adrenaline (3g)	USB	HSPA	Supported	8.4	9.3.2
Adrenaline (LTE) *Firmware Upgrade Required*	USB	HSPA	Supported	8.8	9.3.2
Motorola					

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
A008	Handset	GPRS	Supported	6.7	8.9.1
A630	Handset	GPRS	Supported	6.7	8.9.1
A845	Handset	UMTS	Supported	6.7	8.9.1
M2501	PC Card	FOMA	Supported	6.9	8.9.1
IZAR*	Handset	UMTS	Supported	7.0	8.9.1
KZRZ*	Handset	UMTS	Supported	7.0	8.9.1
KZRZ*	Handset	EVDO	Supported	7.3	8.9.1
RAZR	Handset	EVDO	Supported	7.3	8.9.1
SLVR	Handset	EVDO	Supported	7.3	8.9.1
T280i	Handset	GPRS	Supported	6.7	8.9.1
T720i	Handset	GPRS	Supported	6.7	8.9.1
V60gi	Handset	GPRS	Supported	6.7	8.9.1
V66i	Handset	GPRS	Supported	6.7	8.9.1
V180	Handset	GPRS	Supported	6.7	8.9.1
V220	Handset	GPRS	Supported	6.7	8.9.1
V3 Razr	Handset	GPRS	Supported	7.3	8.9.1
V3Gxx	Handset	UMTS	Supported	7.1	8.9.1
V9m	Handset	EVDO	Supported	7.3	8.9.1
V400	Handset	GPRS	Supported	6.7	8.9.1
V600	Handset	GPRS	Supported	6.7	8.9.1
Volans*	Handset	UMTS	Supported	7.0	8.9.1
Z551	Handset	EDGE	Supported	6.7	8.9.1
Z9	Handset	HSDPA	Supported	7.3	8.9.1
VA76r	Handset	HSDPA	Supported	8.0.2	8.10
QA1	Handset	HSDPA	Supported	8.0.2	8.10
NEC					
232	Handset	GPRS	Supported	6.7	8.9.1
D01NX	PC Card	GPRS	Supported	8.0.2	8.10
D01NE	PC Card	GPRS	Supported	8.0.2	8.10

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
Nokia					
3220	Handset	EDGE	Supported	6.7	8.9.1
BT3600	Handset	GPRS	Supported	6.7	8.9.1
BT3650	Handset	GPRS	Supported	6.7	8.9.1
5100	Handset	GPRS	Supported	6.7	8.9.1
6100	Handset	GPRS/GSM	Supported	6.7	8.9.1
6200	Handset	EDGE	Supported	6.7	8.9.1
6230	Handset	EDGE	Supported	6.7	8.9.1
6234	Handset	UMTS	Supported	7.0	8.9.1
6282	Handset	UMTS/GPRS/GSM	Supported	6.7	8.9.1
6310i	Handset	GPRS	Supported	6.7	8.9.1
6350	Handset	HSDPA	Supported	8.0.2	
6555b*	Handset	GPRS	Supported	7.3	8.9.1
6620	Handset	EDGE	Supported	6.7	8.9.1
6651	Handset	UMTS	Supported	6.7	8.9.1
6750	Handset	GPRS	Supported	8.0.2	8.10
6790	Handset	GPRS	Supported	8.0.2	8.10
6800	Handset	GPRS	Supported	6.7	8.9.1
6820	Handset	EDGE	Supported	6.7	8.9.1
7610	Handset	GPRS	Supported	6.7	8.9.1
8390	Handset	GPRS	Supported	6.7	8.9.1
E50	Handset	UMTS	Supported	7.0	8.9.1
E61	Handset	UMTS	Supported	7.0	8.9.1
E71	Handset	UMTS	Supported	8.0.2	8.10
N73	Handset	UMTS	Supported	7.0	8.9.1
Tarpon	Handset	UMTS	Supported	8.0.2	8.10
Novatel					
C201	PC Card	1xRTT	Supported	6.3.4	8.9.1

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
G100	PC Card	GPRS	Supported	6.7	8.9.1
G301	PC Card	GPRS	Supported	6.7	8.9.1
u520	PC Card	UMTS	Supported	6.7	8.9.1
u530	PC Card	UMTS	Supported	6.7	8.9.1
u630	PC Card	UMTS	Supported	6.7	8.9.1
v620*	PC Card	1xEVDO/1xRTT	Supported	6.3.4	8.9.1
s620*	PC Card	1xEVDO/1xRTT	Supported	6.3.4	8.9.1
S720*	PC Card	1xEVDO/1xRTT	Supported	6.9	8.9.1
U720	USB	EVDO	Supported	6.7	8.9.1
U727	USB	EVDO	Supported	6.9	8.9.1
U730*	USB	HSDPA	Supported	6.7	8.9.1
EM725	Embedded	EVDO	Supported	7.3	8.9.1
EM726	Embedded	EVDO	Supported	7.3	8.9.1
EM727	Embedded	EVDO	Supported	8.0.2	8.10
Expedite	Embedded	EVDO	Supported	9.1	8.10
EX720	ExpressCard	EVDO	Supported	7.4	8.9.1
EV730*	Embedded	HSDPA	Supported	6.7	8.9.1
EU730*	Embedded	HSDPA	Supported	6.7	8.9.1
U740*	PC Card	HSDPA	Supported	6.7	8.9.1
U760	USB	EVDO	Supported	8.0.2	8.10
E760	Embedded	EVDO	Supported	8.0.2	8.10
C777	Express	EVDO	Supported	8.0.2	8.10
EU740*	Embedded	HSDPA	Supported	6.7	8.9.1
XU870*	ExpressCard/ Embedded	HSDPA 3.6	Supported	6.9	8.9.1
U870*	PC Card	HSDPA 3.6	Supported	6.9	8.9.1
EU860D	Embedded	HSDPA 3.6	Supported	7.3	8.9.1
EU870D*	ExpressCard/ Embedded	HSDPA 3.6	Supported	7.1	8.9.1

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
XU950D	ExpressCard/ Embedded	HSDPA 7.2	Supported	7.1	8.9.1
MC950*	ExpressCard/ Embedded	HSDPA 7.2	Supported	7.2	8.9.1
MC950D	ExpressCard/ Embedded	HSDPA 7.2	Supported	7.3	8.9.1
MC990D	USB	HSDPA 7.2	Supported	8.0.2	8.10
U998	USB	EVDO	Supported	8.2	8.10
MiFi2352	USB	WiFi/HSDPA	Supported	8.0.2	8.10
U1000 (Dual mode CDMA/GSM)		CDMA/GSM	Supported	8.1.1	8.10
PC770	Express/PC	CDMA	Supported	8.2	8.10
MC547	USB	CDMA	Supported	8.3.2	8.10
Option					
GT Fusion+ 3G/EDGE*	PC Card	UMTS/WiFi	Supported	6.7	8.9.1
GT Fusion+ HSDPA*	PC Card	GPRS	Supported	6.7	8.9.1
GT Combo EDGE*	PC Card	EDGE	Supported	6.7	8.9.1
GT EDGE*	PC Card	EDGE	Supported	6.7	8.9.1
GT 3G Quad*	PC Card	UMTS	Supported	6.7	8.9.1
GT 3G/EDGE*	PC Card	UMTS	Supported	6.7	8.9.1
GT HSDPA*	PC Card	UMTS	Supported	6.7	8.9.1
GT Max W*	PC Card	HSDPA	Supported	6.7	8.9.1
GT Max E*	PC Card	HSDPA	Supported	6.7	8.9.1
GT Max J*	PC Card	HSDPA	Supported	6.7	8.9.1
GT Max 7.2 Ready E	PC Card	HSDPA	Supported	6.7	8.9.1
GT Max 7.2 Ready W	PC Card	HSDPA	Supported	6.7	8.9.1

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
GT Express 7.2 E*	PC Card	HSDPA 7.2	Supported	7.1	8.9.1
GT Express 7.2 W*	PC Card	HSDPA 7.2	Supported	7.1	8.9.1
GT Express HSUPA E*	PC Card	HSUPA	Supported	7.0	8.9.1
GT Express HSUPA W*	PC Card	HSUPA	Supported	7.0	8.9.1
GT Express 401	PC Card	HSUPA	Certified	7.4	8.9.1
3G*	PC Card	UMTS	Supported	6.9	8.9.1
GT*	PC Card	HSDPA/EDGE	Supported	6.9	8.9.1
GTM 351 E*	Embedded	HSDPA	Supported	6.9	8.9.1
GTM 378	Embedded	HSDPA 3.6	Supported	7.3	8.9.1
GTM 380 E*	Embedded	HSDPA 7.2	Supported	7.1	8.9.1
GTM 380 W*	Embedded	HSDPA 7.2	Supported	7.1	8.9.1
GTM 382	Embedded	HSDPA 7.2	Supported	8.0.2	8.10
GS Icon*	USB	HSDPA	Supported	6.9	8.9.1
GS 401	USB	HSDPA	Certified	7.4	8.9.1
GS Icon 7.2 E*	USB	HSDPA 7.2	Supported	7.1	8.9.1
GS Icon 3	USB	HSDPA 7.2	Certified	7.4	8.9.1
GT GTM378 E*	Embedded	HSDPA 3.6/7.2	Supported	7.0	8.9.1
GT GE 201/202*	ExpressCard	HSDPA 7.2	Supported	7.3	8.9.1
GT GE 301/302*	ExpressCard	HSDPA 7.2	Supported	7.3	8.9.1
GS GI 301/302*	USB	HSUPA	Supported	7.2	8.9.1
E3730	ExpressCard	HSUPA	Supported	8.1.1	8.10
GTM 378	Embedded	HSDPA 3.6 / 7.2	Supported	7.3	8.9.1
Icon 322	USB	HSDPA 7.2	Supported	8.0.2	8.10
GI0505	USB	HSDPA	Supported	8.0.2	8.10
GE441	USB	HSDPA	Supported	8.0.2	8.10
Icon 461	USB	HSDPA	Supported	8.0.2	8.10
Palm					

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
Treo 750v*	Handset	GPRS	Supported	7.0	8.9.1
Pantech					
C810*	Handset	HSDPA	Supported	7.3	8.9.1
PX-500	PC Card	1xEVDO Rev A/ 1xRTT	Supported	7.4	8.9.1
5740	PC Card	1xEVDO/1xRTT	Supported	7.3	8.9.1
5750	PC Card	1xEVDO/1xRTT	Supported	7.3	8.9.1
C630	Handset	HSDPA	Supported	8.0.2	8.10
C610	Handset	HSDPA	Supported	8.0.2	8.10
UM175AL	USB	EVDO	Supported	8.1	8.10
Qualcomm					
GOBI*	Embedded	HSUPA	Certified	7.3	8.9.1
GOBI*	Embedded	1xEVDO/1xRTT	Supported	8.0.2	9.3.2
GOBI	Embedded	EVDO	Supported	8.0.2	9.3.2
GOBI 2000*	Embedded	HSUPA	Certified	8.0.2	9.3.2
GOBI 2000*	Embedded	EVDO	Certified	8.0.2	9.3.2
GOBI 3000*	Embedded	LTE[17]/EVDO/HSPA	Supported	8.8	
RIM					
7130c	Handset	GPRS	Supported	6.7	8.9.1
7135v	Handset	GPRS	Supported	6.7	8.9.1
7100g	Handset	GPRS	Supported	6.7	8.9.1
7290	Handset	GPRS	Supported	6.7	8.9.1
7250	Handset	1xEVDO/1xRTT	Supported	6.7	8.9.1
7250v	Handset	GPRS	Supported	6.9	8.9.1
8100v	Handset	GPRS	Supported	7.0	8.9.1
8110	Handset	GPRS	Supported	8.0.2	8.10
8120	Handset	EDGE	Supported	7.3	8.9.1

[17] LTE is a trademark of ETSI

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
8130	Handset	EVDO	Pending	8.2	8.10
8230	Handset	EVDO	Pending	8.2	8.10
8300*	Handset	EDGE	Supported	7.3	8.9.1
8320	Handset	EDGE	Supported	8.0.2	8.10
8300v	Handset	UMTS	Supported	7.3	8.9.1
8300c	Handset	UMTS	Supported	7.3	8.9.1
8300	Handset	EVDO	Supported	7.3	8.9.1
8330	Handset	UMTS	Supported	8.0.2	8.10
8520	Handset	UMTS	Supported	8.0.2	8.10
8530	Handset	CDMA	Pending	8.3.2	8.10
8703	Handset	UMTS	Supported	8.0.2	8.10
8700v	Handset	GPRS	Supported	6.9	8.9.1
8707v	Handset	UMTS	Supported	6.9	8.9.1
8830	Handset	EVDO	Supported	7.3	8.9.1
8900	Handset	GPRS	Supported	8.0.2	8.10
9000	Handset	GPRS	Certified	7.4	8.9.1
9300	Handset	GPRS	Pending	8.3.2	8.10
9630	Handset	EVDO	Pending	8.3.2	8.10
9650	Handset	EVDO	Pending	8.3.2	8.10
9700	Handset	GPRS	Certified	8.0.2	8.10
9700a	Handset	GPRS	Pending	8.2	8.10
9800	Handset	HSDPA/EDGE	Certified	8.1.2	8.10
Samsung					
A900M	Handset	EVDO	Supported	7.3	8.9.1
E317	Handset	GPRS	Supported	6.7	8.9.1
m300	Handset	EVDO	Supported	7.3	8.9.1
m500	Handset	EVDO	Supported	7.3	8.9.1
m510	Handset	EVDO	Supported	7.3	8.9.1
m540	Handset	EVDO	Supported	8.0.2	8.10

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
m620	Handset	EVDO	Supported	7.3	8.9.1
m630	Handset	EVDO	Supported	8.0.2	8.10
SGH-A727*	Handset	UMTS	Supported	7.0	8.9.1
SGH-A747	Handset	HSDPA	Supported	7.3	8.9.1
SGH-i617*	Handset	HSDPA	Supported	7.3	8.9.1
SGH-i627	Handset	HSDPA	Supported	8.0.2	8.10
SGH-i637	Handset	HSDPA	Supported	8.0.2	8.10
SGH-A737*	Handset	EDGE	Supported	7.3	8.9.1
SGH-A837	Handset	EDGE	Supported	8.0.2	8.10
S105	Handset	GPRS	Supported	6.7	8.9.1
S307	Handset	GPRS	Supported	6.7	8.9.1
SGH300	Handset	GPRS	Supported	6.7	8.9.1
SGH-ZV50	Handset	GPRS	Supported	7.0	8.9.1
SGH-Z560V	Handset	GPRS	Supported	7.0	8.9.1
SGH-Z700	Handset	EVDO	Supported	7.3	8.9.1
SPH-900	Handset	EVDO	Supported	7.3	8.9.1
SPH-920	Handset	EVDO	Supported	7.3	8.9.1
ZX10	Handset	UMTS	Supported	6.7	8.9.1
ZX20	Handset	UMTS	Supported	6.7	8.9.1
i907	Handset	UMTS	Supported	8.0.2	8.10
SGH-A867	Handset	UMTS	Supported	8.0.2	8.10
SGH-A767	Handset	UMTS	Supported	8.0.2	8.10
SGH-A777	Handset	UMTS	Supported	8.0.2	8.10
SGH-A797	Handset	UMTS	Supported	8.0.2	8.10
SGH-A877	Handset	UMTS	Supported	8.0.2	8.10
SGH-A657	Handset	UMTS	Supported	8.0.2	8.10
SGH-A887	Handset	UMTS	Supported	8.0.2	8.10
SGH-A897	Handset	UMTS	Supported	8.0.2	8.10
NC10	Embedded	HSDPA	Supported	8.0.2	8.10

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
NC20	Embedded	HSDPA	Supported	8.0.2	8.10
Y3100	Embedded	HSDPA	Certified	8.0.2	8.10
Y3300	Embedded	HSDPA	Supported	8.1	8.10
N150	Embedded	HSDPA	Supported	8.1	8.10
Sanyo					
Katana DLX	Handset	EVDO	Supported	7.3	8.9.1
Katana LX	Handset	EVDO	Supported	7.3	8.9.1
Pro 200	Handset	EVDO	Supported	7.3	8.9.1
Pro 700	Handset	EVDO	Supported	7.3	8.9.1
S1	Handset	EVDO	Supported	7.3	8.9.1
SCP-3100	Handset	EVDO	Supported	7.3	8.9.1
SCP-3200	Handset	EVDO	Supported	7.3	8.9.1
SCP-6650	Handset	EVDO	Supported	7.3	8.9.1
SCP-7050	Handset	EVDO	Supported	7.3	8.9.1
SCP-8400	Handset	EVDO	Supported	7.3	8.9.1
SCP-M1	Handset	EVDO	Supported	7.3	8.9.1
Seiko					
VC701SI*	PC Card	UMTS	Supported	6.7	8.9.1
Siemens					
C61	Handset	GPRS	Supported	6.7	8.9.1
CT56	Handset	GPRS	Supported	6.7	8.9.1
CT66	Handset	GPRS	Supported	6.7	8.9.1
P207	Handset	EDGE	Supported	6.7	8.9.1
P777	Handset	EDGE	Supported	6.7	8.9.1
S46	Handset	GPRS	Supported	6.7	8.9.1
S55	Handset	GPRS	Supported	6.7	8.9.1
S56	Handset	GPRS	Supported	6.7	8.9.1
SL56	Handset	GPRS	Supported	6.7	8.9.1
Sierra Wireless					

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
Aircard 550	PC Card	1xRTT	Supported	6.7	8.9.1
Aircard 555	PC Card	1xRTT	Supported	6.7	8.9.1
Aircard 580	PC Card	1xEVDO/1xRTT	Supported	6.7	8.9.1
Aircard 595	PC Card	EVDO RevA	Supported	7.0	8.9.1
Aircard 595u	USB	EVDO RevA	Supported	7.1	8.9.1
Aircard C597	ExpressCard	EVDO RevA	Supported	7.1	8.9.1
Aircard 597e	ExpressCard	EVDO RevA	Supported	7.1	8.9.1
Aircard C598	USB	EVDO	Supported	8.0.2	
Aircard 710	PC Card	GPRS	Supported	6.7	8.9.1
Aircard 750	PC Card	GPRS	Supported	6.7	8.9.1
Aircard 775	PC Card	EDGE	Supported	6.4	8.9.1
Aircard 850*	PC Card	HSDPA	Supported	6.7	8.9.1
Aircard 860	PC Card	HSDPA	Supported	6.5	8.9.1
Aircard 875	PC Card	HSDPA	Supported	6.9	8.9.1
Aircard 875u	USB	HSDPA	Supported	7.1	8.9.1
Aircard 881	PC Card	HSDPA 7.2	Supported	7.1	8.9.1
Aircard 881u	USB	HSDPA 7.2	Supported	7.3	8.9.1
Airprime 3200	PC Card	1xRTT	Supported	6.7	8.9.1
Airprime 3300	PC Card	1xRTT	Supported	6.7	8.9.1
Airprime 5220	PC Card	1xEVDO	Supported	6.7	8.9.1
HS2300	Embedded	HSDPA	Supported	9.1	
MC5725	Embedded	EVDO	Supported	7.3	8.9.1
MC5727	Embedded	EVDO	Certified	7.4	8.9.1
MC5728	Embedded	EVDO	Supported	8.0.2	8.10
MC7700[18]	Embedded	LTE[19]/HSPA+	Certified	8.8	
MC7500[20]	Embedded	LTE/EVDO/HSPA+	Supported	8.8	

[18] The MC7700 is only approved for the AT&T 4G LTE network.
[19] LTE is a trademark of ETSI
[20] The MC7750 is only approved for the Verizon 4G LTE Network.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
MC8755	Embedded	HSDPA	Supported	6.7	8.9.1
MC8765	Embedded	HSDPA	Supported	6.7	8.9.1
MC8775	Embedded	HSDPA 3.6	Supported	6.7	
MC8780	Embedded	HSDPA 7.2	Supported	7.1	8.9.1
MC8781	Embedded	HSUPA	Supported	7.3	9.3.2
MC8790	Embedded	HSUPA	Certified	8.0.2	8.10
C885	USB	HSUPA	Certified	7.4	8.9.1
AC402	ExpressCard	EVDO	Certified	8.0.2	8.10
USB305	USB	HSUPA	Supported	8.0.2	8.10
USBConnect Lightning	USB	HSUPA	Certified	8.1	8.10
USB306	USB	HSUPA	Supported	8.0.2	8.10
AC 890	USB	HSPA	Certified	8.0.3	8.10
AC 250U	USB	CDMA	Supported	8.2	9.3.2
USB308	USB	HSPA+	Certified	8.3.2	9.3.2
Sprint Branded					
T598	???	CDMA	Supported	8.11	
Softbank					
C01SI	ExpressCard	HSDPA 3.6	Supported	8.0.2	8.10
Sony Ericsson					
K800	Handset	HSDPA	Supported	7.0	8.9.1
M600/M600i	Handset	HSDPA	Supported	7.0	8.9.1
T68i	Handset	GPRS	Supported	6.7	8.9.1
T300	Handset	GPRS	Supported	6.7	8.9.1
T310	Handset	GPRS	Supported	6.7	8.9.1
T316	Handset	GPRS	Supported	6.7	8.9.1
T610	Handset	GPRS	Supported	6.7	8.9.1
T616	Handset	GPRS	Supported	6.7	8.9.1
T637	Handset	GPRS	Supported	6.7	8.9.1

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
S710	Handset	EDGE	Supported	6.7	8.9.1
P800	Handset	GPRS	Supported	6.7	8.9.1
P990i	Handset	UMTS	Supported	7.0	8.9.1
W200i	Handset	HSDPA	Supported	7.1	8.9.1
Z500a	Handset	GPRS	Supported	6.7	8.9.1
GC75	PC Card	GPRS	Supported	7.4	8.9.1
GC79	PC Card	GPRS/WiFi	Supported	6.7	8.9.1
GC82	PC Card	EDGE	Supported	6.7	8.9.1
GC83	PC Card	EDGE	Supported	6.7	8.9.1
GC85	PC Card	EDGE	Supported	7.4	8.9.1
GC89	PC Card	EDGE/WiFi	Supported	6.7	8.9.1
GC89c	PC Card	EDGE/WiFi	Supported	6.7	8.9.1
EC400	ExpressCard	HSDPA	Supported	7.4	8.9.1
W760	Handset	HSDPA	Supported	8.0.2	8.10
Bear	Handset	HSDPA	Supported	8.0.2	8.10
W518a	Handset	HSDPA	Supported	8.0.2	8.10
C905	Handset	HSDPA	Supported	8.0.2	8.10
TimesPower					
WM2080B	PC Card	UMTS	Supported	6.9	8.9.1
UT StarComm					
PC-5740SP	PC Card	UMTS	Supported	6.3.4	8.9.1
PC-5750SP	PC Card	UMTS	Supported	6.7	8.9.1
UM100	USB	EVDO	Supported	8.0.2	8.10
UM150	USB	EVDO	Supported	8.0.2	8.10
UM175	USB	EVDO	Supported	8.0.2	8.10
GTX75	Handset	UMTS	Supported	8.0.2	8.10
Verizon Branded					
USB760	USB	CDMA	Supported	8.11	
Vodafone					

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

DEVICE	DEVICE TYPE	TECHNOLOGY	STATUS[16]	MINIMUM VERSION	LAST SUPPORTED AT&T GLOBAL NETWORK CLIENT VERSION
Pebble	USB	HSDPA	Supported	7.3	8.9.1
Pebble	USB	HSDPA 7.2	Supported	7.3	8.9.1
Pebble	USB	HSDPA 7.2	Supported	7.3	8.9.1
Anaconda	USB	HSDPA	Supported	7.3	8.9.1
Vodafone VPA Compact III	Handset	UMTS	Supported	7.0	8.9.1
ZTE					
MF626	USB	HSPA (HSDPA)	Supported	8.0.2	8.10
MF630	USB	HSPA (HSDPA)	Supported	7.2	8.9.1
MF633r	USB	HSPA (HSDPA)	Certified	8.0.2	8.10
MF636	USB	HSPA (HSDPA)	Supported	8.3.2	8.10
MF180	USB	HSPA (HSDPA)	Supported	8.3.2	8.10
MF668	USB	HSPA (HSDPA)	Supported	8.3.2	8.10
MZ29	USB	HSDPA	Certified	7.3	8.9.1
MZ10	USB	HSDPA	Certified	7.4	8.9.1
MZ628	USB	HSDPA	Supported	7.4	8.9.1
K3520-Z	USB	HSDPA	Certified	7.4	8.9.1
K3565-Z	USB	HSDPA	Supported	8.0.2	8.10
K3570-Z	USB	HSDPA	Supported	8.1	8.10
K3571-Z	USB	HSDPA	Supported	8.1	8.10
K3765-Z	USB	HSDPA	Supported	8.0.2	8.10
K4505-Z	USB	HSDPA	Supported	8.0.2	8.10
K3805-Z	USB	HSDPA	Certified	8.0.2	8.10
K3806-Z	USB	HSDPA	Supported	8.2	8.10

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Appendix C: Third-Party Firewall Support

Network Firewalls

You may need to alter your network firewall configuration to allow AT&T Global Network Client management and VPN traffic to route properly. The table below lists the required changes.

Source	Dest	Protocol Port Source	Protocol Port Dest	Action	Reason for opening
ALL SERVICES					
Local PC	144.160.245.70	TCP:1024 +	HTTP:80	Allow	SLA Data collector
Local PC	144.160.245.71	TCP:1024 +	HTTP:80	Allow	SLA Data collector
Local PC	32.97.166.118	TCP:1024 +	HTTP:80	Allow	Hotspot Directory Updates
Local PC	SMX List	TCP:1024 +	HTTP:80 (443)	Allow	Authentication
Local PC	165.87.194.246	TCP:1024 +	TCP:21	Allow	Passive FTP for AGNC, Certificate and Firmware updates
IPSec					
Local PC	VPN Gateways IPs	ESP (50)	ESP (50)	Allow	IPSec
VPN Gateways IPs	Local PC	ESP (50)	ESP (50)	Allow	IPSec
Local PC	VPN Gateways IPs	UDP:500	UDP:500,	Allow	IPSec (IKE)
VPN Gateways IPs	Local PC	UDP:500	UDP:500,	Allow	IPSec (IKE)
Local PC	VPN Gateways IPs	UDP:1024+	UDP 4500	Allow	IPSec with NAT Traversal

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

VPN Gateways Ips	Local PC	UDP 4500	UDP:1024+	Allow	IPSec with NAT Traversal
AT&T Network-Based IP VPN Remote Access service					
Local PC	VPN Gateways IPs	UDP:1024+	UDP:5080	Allow	AT&T VIG Server Health Check

SSLT					
Local PC	VPN Gateways IPs	TCP:1024 +	TCP:443	Allow	SSL

Figure 51: Network Firewall Configuration Table

SMiX List

Last Updated 5/9/2013

Name	Region	Location	Secure Address	Internet Address
US01R	US	Allen, Tx	32.96.129.227	204.146.172.225
US02R	US	Redwood City, CA	32.96.129.234	204.146.166.105
US03R	US	Allen, Tx	32.96.129.228	204.146.172.226
US04R	US	Redwood City, CA	32.96.129.242	204.146.219.1
US05R	US	Ashburn, VA		12.67.9.6
US06R	US	Ashburn, VA		12.67.9.9
US21R	US	Allen, Tx	32.96.129.230	204.146.172.230
US22R	US	Redwood City, CA	32.96.129.237	204.146.166.107
US25R	US	Ashburn, VA		12.67.9.15
GB02R	EMEA	London	32.239.254.6	152.158.16.57

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

GB03R	EMEA	London	32.227.63.185	32.112.51.115
DE02R	EMEA	Frankfurt	32.239.254.22	152.158.2.57
DE03R	EMEA	Frankfurt	32.227.64.184	32.112.50.131
NL02R	EMEA	Amsterdam		195.212.144.20
NL03R	EMEA	Amsterdam	32.224.251.20	195.212.144.21
HK01R	AP	Hong Kong	32.233.96.248	122.248.141.244
HK02R	AP	Hong Kong	32.233.96.247	122.248.141.245
JP01R	AP	Osaka	32.233.96.254	210.88.144.203
JP02R	AP	Tokyo	32.233.96.253	210.88.144.155
JP03R	AP	Tokyo	32.233.96.252	210.88.1.199
JP04R	AP	Osaka	32.233.96.251	210.88.144.43

Figure 52: SMiX Address Table

Personal/Client Firewalls

The AT&T Global Network Client program uses IP to communicate with other computers on the network just like other network programs (such as web browsers and e-mail programs). Third-party personal firewalls can prohibit certain types of network communication. Running multiple firewalls on users' PCs can cause difficulties and is not supported by AT&T.

Some firewalls must be configured to allow the AT&T Global Network Client to communicate with the network in order for client features to function properly. The table below lists the required changes. More information about the features is found in the list below the table.

Feature	Protocol: Port
Dial Authentication	TCP:5053
Disconnect Warning	UDP:7000
Software Updates	TCP:20,21

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

SLA Data Collection, Configuration Settings	HTTP/TCP:80

Figure 53: Client Firewall Configuration Table

Dial Authentication

The AT&T Global Network Client uses a proprietary enhanced authentication process using TCP:5053.

A customization could be made to the AT&T Global Network Client to disable enhanced authentication and use PAP, but it is not recommended. If disabled, the following consequences would occur:

- Meaningful error messages are lost. Instead of "invalid user ID", "expired password", "revoked password", etc. the user only sees "authentication failed."
- Login retries are lost. The user must redial to change user ID or password.
- The ability to warn a user if a closer access number is available is lost.
- Ability to change passwords is lost.
- The AT&T helpdesk will not provide first-level support without special arrangements

Disconnect warning

The AT&T Global Network Client communicates with the dialed gateway after connecting using UDP port 7000 to be notified of pending disconnects. Disconnect time limits are configured in the AT&T administration server. If the connection is idle for the specified amount of time a datagram is sent from the gateway to the AT&T Global Network Client and the AT&T Global Network Client displays a warning that the connection will be disconnected in 1 minute unless the user takes the appropriate action.

Maximum inactivity timeouts are set in the AT&T Configuration Server at the account level. The AT&T gateways will timeout inactive connections regardless of the remote access software used. The warning will only be displayed if the AT&T Global Network Client is allowed to communicate on UDP port 7000.

Software updates

The AT&T Global Network Client periodically checks for and downloads updates to the software using anonymous FTP (TCP ports 20 and 21).

SLA data collection

The AT&T Global Network Client uploads data about all connection attempts using HTTP (TCP port 80) to a server after connecting. This data is used for measuring SLAs (Service Level Agreements). If the SLA data is not collected, AT&T will not provide service-level guarantees.

AT&T requires companies to add policy rules to their firewalls to allow SLA data to be sent to those servers.

Configuration Updates

The AT&T Global Network Client requests configuration settings (like start page, e-mail server, proxy server, etc) from an AT&T administration server. The AT&T Global Network Client updates third-party e-

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

mail and browser programs with these settings. AT&T recommends adding policy rules to the firewall to allow updates to be retrieved.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Appendix D: Using the Command Line Program

The AT&T Global Network Client can be started using the command line program. This program accepts the following command-line parameters:

AT&T Client

netclient.exe [-connect] [-login=LoginProfile] [-password=Password]

netclient.exe [-login=LoginProfile] [-password=Password]

netclient.exe [-exit | -exitnow]

netclient.exe [-disconnect | -disconnect]

netclient.exe [-help]

netclient.exe [-initonly]

netclient.exe [-password=Password]

netclient.exe [-timeout=[IdleTime] [,[DurationTime] [,[ThresholdTime] [,[ThresholdBytes] [,WarnTime]]]]]

Parameters[21]:

-connect

Displays the Login window and starts a connection if the password is saved or if the password is entered as a command-line parameter (-password).

-disconnect

Disconnects after prompting for confirmation if necessary.

-disconnectnow

Disconnects with no confirmation.

[21] Note: Some of these parameters can be combined on the same command-line (for example 'netclient.exe -connect -login="my Internet login"'.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

-exit

Closes this program and prompts for confirmation before disconnecting if necessary.

-exitnow

Closes this program with no confirmation before disconnecting.

-getstatus

Returns a code to indicate the state of this program. This parameter is only useful when invoked from a program that can interpret the return code.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Status codes returned by –getstatus:

NotRunning	0
Initializing	100
NotConnected	200
BeforeConnecting	300
BeforeConnectAttempt	350
VerifyExistingInternetConnection	370
VerifyExistingProxyConnection	375
BeforeDialing	400
Dialing	500
AuthenticatingDial	600
AfterDialing	700
BeforeCellularSDKConnect	710
ConnectingCellularSDK	712
AuthenticatingCellularWIG	714
AfterCellularSDKConnect	716
BeforeWiFiConnect	720
ConnectingWiFi	730
AuthenticatingWiFi	740
AfterWiFiConnect	750
BeforeEthernetConnect	756
AuthenticatingEthernet	758
AfterEthernetConnect	760
PauseWhileConnectingForTesting	765
Phase1Authenticate	770
NoPhase1OrPhase2Needed	780
BeforeTunneling	800
Tunneling	900
AuthenticatingTunnel	1000

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

AfterTunneling	1100
AfterConnecting	1200
ConnectedNoVPN	1250
ReattachingToVPNServer	1270
AfterReattachingToVPNServer	1275
Connected	1300
BeforeDisconnecting	1400
Disconnecting	1500
AfterDisconnecting	1600
Disconnected	1700
Exiting	1800

-help

Displays this help window.

-initonly

Initializes the database after a new install and then exits.

-login=LoginProfile

The specified LoginProfile is made the current login profile. If LoginProfile contains spaces it should be enclosed in double-quotes (for example: -login="my Internet login").

-password=Password

Sets the password for the current login profile, as if Password was entered on the Login window.

-timeout

Changes the timeout properties. Five separate parameters may be included an idle time, a duration time, a threshold time, threshold bytes and a timeout warning time. All of the times are in seconds. See Timeout Options for a description of these options. Any of the five parameters can be left empty to indicate no change or set to zero to disable the timeout. Invalid values will be ignored.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

NOTE: The idle-timeout parameter has become obsolete and is ignored in version 7.6 and higher. The idle-timeout parameter was left in place to remain compatible with other programs that previously passed that parameter.

Examples:

netclient.exe -timeout=,,,,0

Leave the timeouts unchanged but disable the timeout warning.

netclient.exe -timeout=,3600,,,60

Set a duration timeout of 1 hour and display a warning 1 minute before disconnecting.

AT&T Global Network Client Firewall

netfw.exe[-firewall=on|off]

Parameters:

-firewall=on|off

Turns AT&T Global Network Client Firewall on or off.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Appendix E: AT&T T6 Client

The T6 Client is part of the AT&T IPv6 Service. Customers with the T6 Client installed on their PC will be able to reach IPv6 network and content through AT&T IPv6 Service. If IPv6 is not available, applications will default to IPv4.

Corporate Networks

The T6 Service is a tunneling protocol which needs to access specific (configurable) UDP ports. On some corporate networks, these ports are blocked, and therefore the T6 service will not work.

Operating Systems

- Windows Vista (SP1)
- Windows 7
- (Windows 8 is not supported)

Components of the T6 Client

- T6 Client Service – creates a tunnel to the IPv6 gateway to send/receive messages
- T6 UI or Tray Icon – Allows users to interact with the T6 service by clicking the icon and selecting a displayed option
- Mini-port Driver for the T6 Client - Interface (virtual adapter) that allows the T6 Client to interact with the network

System Tray Icon

After installation, a T6 icon will be present in the system tray. There will be three colors associated with this icon (see below), as well as a menu accessed by clicking on the icon. Hovering over the T6 icon will result in informational messages being presented.

A "blue" icon represents that the T6 tunnel is active with an IPv6 address assigned

Figure 54: Blue T6 Client Icon

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

A "yellow" icon represents that there is no active tunnel with an IPv6 address assigned, however the T6 service may be actively trying to establish a tunnel. The T6 Client will poll the T6 gateway every ninety seconds. If no response is received, it will attempt to connect to an alternate T6 gateway. This may take a few minutes before a new connection is established.

Figure 55: Yellow T6 Client Icon

A "grey" icon represents that the T6 service is stopped and there is no IPv6 tunnel.

Figure 56: Grey T6 Client Icon

Software Updates

The T6 Client will automatically check for a software update every day. If an update is available, a message will be displayed when hovering you mouse over the T6 tray icon. Clicking Install Update from the Tray Icon Menu will proceed to install the advertised update.

Figure 57: T6 Client Software update

Tray Icon Menu

Clicking on the T6 Service icon in the system tray will display several categories the user can choose to access.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Figure 58: T6 Client Tray Icon Menu

AT&T T6 Service and Options allows you to stop and restart the T6 Tunnel service. If the service is stopped or the tray icon does not turn blue, click on the Start or Restart button.

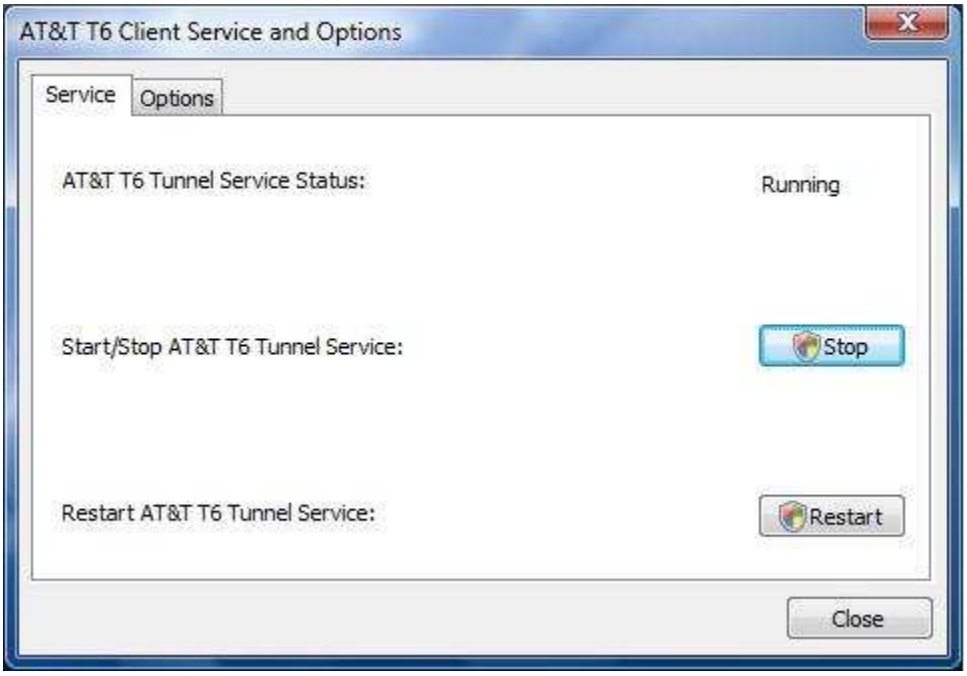


Figure 59: T6 Client Menu Options

The Options tab will allow the user to enable and disable the T6 service to tunnel IPv6.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

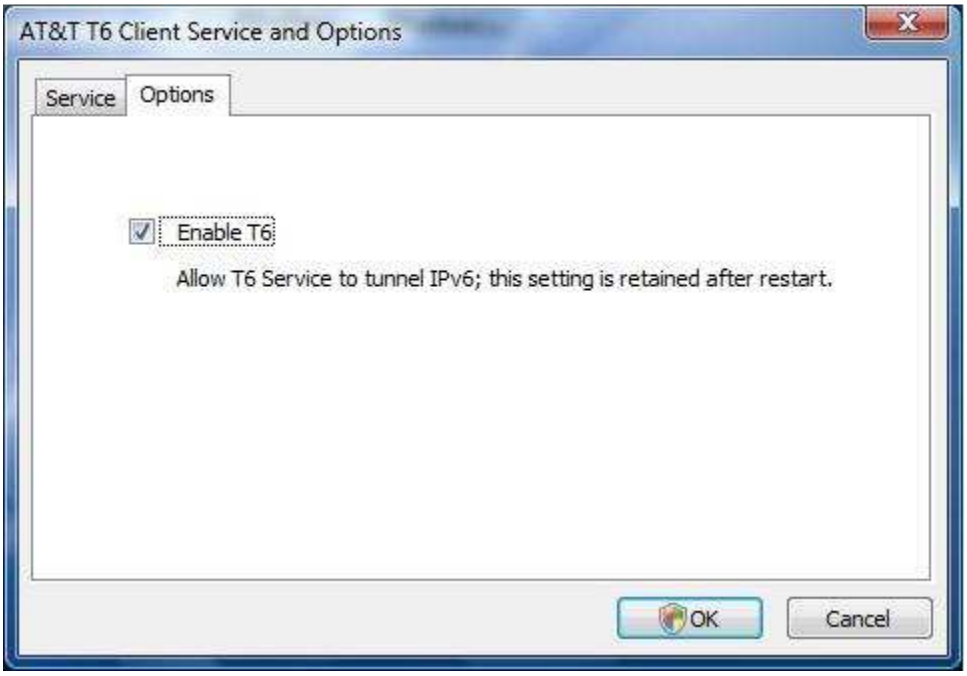


Figure 60: T6 Client Enable Option

Network Information gives the viewer detailed information regarding their computer's network.

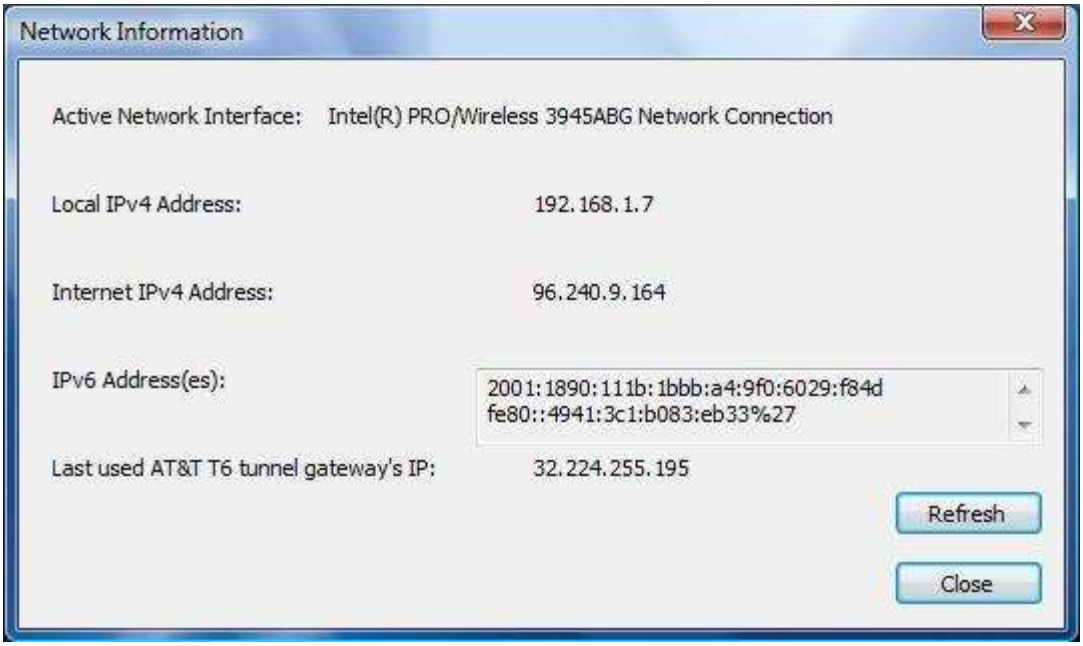


Figure 61: T6 Client Network Information

About AT&T T6 Client will provide version and copyright information of the product.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Figure 62: About the AT&T T6 Client

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Open History File will display the T6 Client entry log from installation through current time and may be used to track events associated with the T6 service.

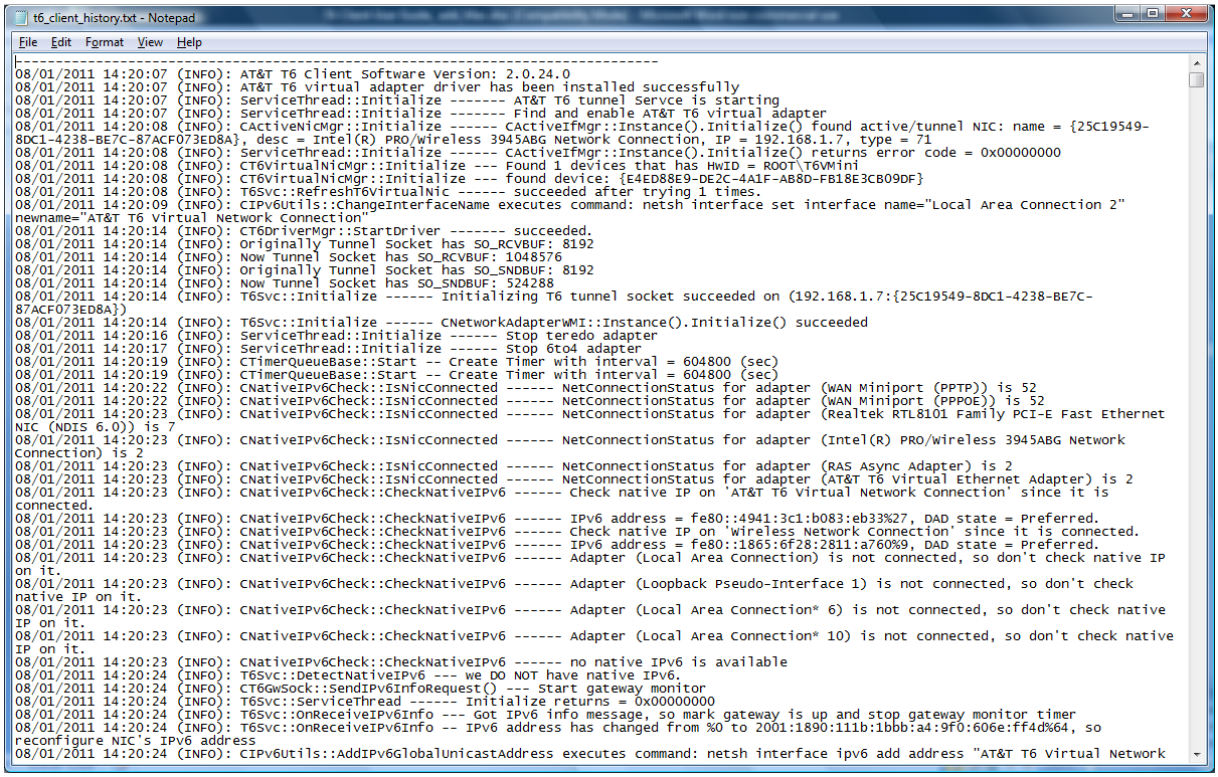

t6_client_history.txt - Notepad
File Edit Format View Help
08/01/2011 14:20:07 (INFO): AT&T T6 Client Software Version: 2.0.24.0
08/01/2011 14:20:07 (INFO): AT&T T6 virtual adapter driver has been installed successfully
08/01/2011 14:20:07 (INFO): ServiceThread::Initialize ------- AT&T T6 tunnel Servce is starting
08/01/2011 14:20:07 (INFO): ServiceThread::Initialize ------- Find and enable AT&T T6 virtual adapter
08/01/2011 14:20:08 (INFO): CActiveNicMgr::Initialize ------ CActiveIfMgr::Instance().Initialize() found active/tunnel NIC: name = {25C19549-8DC1-4238-BE7C-87ACF073ED8A}, desc = Intel(R) PRO/Wireless 3945ABG Network Connection, IP = 192.168.1.7, type = 71
08/01/2011 14:20:08 (INFO): ServiceThread::Initialize ------ CActiveIfMgr::Instance().Initialize() returns error code = 0x00000000
08/01/2011 14:20:08 (INFO): CT6VirtualNicMgr::Initialize --- Found 1 devices that has HwID = ROOT\T6VMini
08/01/2011 14:20:08 (INFO): CT6VirtualNicMgr::Initialize --- found device: {E4ED88E9-DE2C-4A1F-AB8D-FB18E3CB09DF}
08/01/2011 14:20:08 (INFO): T6Svc::RefreshT6VirtualNic ------ succeeded after trying 1 times.
08/01/2011 14:20:09 (INFO): CIPv6Utils::ChangeInterfaceName executes command: netsh interface set interface name="Local Area Connection 2" newname="AT&T T6 Virtual Network Connection"
08/01/2011 14:20:14 (INFO): CT6DriverMgr::StartDriver ------- succeeded.
08/01/2011 14:20:14 (INFO): Originally Tunnel Socket has SO_RCVBUF: 8192
08/01/2011 14:20:14 (INFO): Now Tunnel Socket has SO_RCVBUF: 1048576
08/01/2011 14:20:14 (INFO): Originally Tunnel Socket has SO_SNDBUF: 8192
08/01/2011 14:20:14 (INFO): Now Tunnel Socket has SO_SNDBUF: 524288
08/01/2011 14:20:14 (INFO): T6Svc::Initialize ------ Initializing T6 tunnel socket succeeded on (192.168.1.7:{25C19549-8DC1-4238-BE7C-87ACF073ED8A})
08/01/2011 14:20:14 (INFO): T6Svc::Initialize ------ CNetworkAdapterWMI::Instance().Initialize() succeeded
08/01/2011 14:20:16 (INFO): ServiceThread::Initialize ------ Stop teredo adapter
08/01/2011 14:20:17 (INFO): ServiceThread::Initialize ------ Stop 6to4 adapter
08/01/2011 14:20:19 (INFO): CTimerQueueBase::Start -- Create Timer with interval = 604800 (sec)
08/01/2011 14:20:19 (INFO): CTimerQueueBase::Start -- Create Timer with interval = 604800 (sec)
08/01/2011 14:20:22 (INFO): CNativeIPv6Check::IsNicConnected ------ NetConnectionStatus for adapter (WAN Miniport (PPTP)) is 52
08/01/2011 14:20:22 (INFO): CNativeIPv6Check::IsNicConnected ------ NetConnectionStatus for adapter (WAN Miniport (PPPOE)) is 52
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::IsNicConnected ------ NetConnectionStatus for adapter (Realtek RTL8101 Family PCI-E Fast Ethernet NIC (NDIS 6.0)) is 7
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::IsNicConnected ------ NetConnectionStatus for adapter (Intel(R) PRO/Wireless 3945ABG Network Connection) is 2
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::IsNicConnected ------ NetConnectionStatus for adapter (RAS Async Adapter) is 2
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::IsNicConnected ------ NetConnectionStatus for adapter (AT&T T6 Virtual Ethernet Adapter) is 2
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ Check native IP on 'AT&T T6 Virtual Network Connection' since it is connected.
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ IPv6 address = fe80::4941:3c1:b083:eb33%27, DAD state = Preferred.
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ Check native IP on 'Wireless Network Connection' since it is connected.
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ IPv6 address = fe80::1865:6f28:2811:a760%9, DAD state = Preferred.
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ Adapter (Local Area Connection) is not connected, so don't check native IP on it.
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ Adapter (Loopback Pseudo-Interface 1) is not connected, so don't check native IP on it.
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ Adapter (Local Area Connection* 6) is not connected, so don't check native IP on it.
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ Adapter (Local Area Connection* 10) is not connected, so don't check native IP on it.
08/01/2011 14:20:23 (INFO): CNativeIPv6Check::CheckNativeIPv6 ------ no native IPv6 is available
08/01/2011 14:20:24 (INFO): T6Svc::DetectNativeIPv6 --- we DO NOT have native IPv6.
08/01/2011 14:20:24 (INFO): CT6GwSock::SendIPv6InfoRequest() --- Start gateway monitor
08/01/2011 14:20:24 (INFO): T6Svc::ServiceThread ------ Initialize returns = 0x00000000
08/01/2011 14:20:24 (INFO): T6Svc::OnReceiveIPv6Info --- Got IPv6 info message, so mark gateway is up and stop gateway monitor timer
08/01/2011 14:20:24 (INFO): T6Svc::OnReceiveIPv6Info -- IPv6 address has changed from %0 to 2001:1890:111b:1bbb:a4:9f0:606e:ff4d%64, so reconfigure NIC's IPv6 address
08/01/2011 14:20:24 (INFO): CIPv6Utils::AddIPv6GlobalUnicastAddress executes command: netsh interface ipv6 add address "AT&T T6 Virtual Network

Figure 63: T6 Client Entry Log

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Index

A

Access Control List, 87
Accessibility Features, 75
AGN Filter Driver, 20
AT&T Administration Server, 101
AT&T Authentication Server, 13
AT&T Business Internet Services (BIS), 76
AT&T Client Installation Package, 18
AT&T Global Network Client Firewall, 12, 85
  Disabling, 86
  FIREWALL_STATE public property, 67
  Operating Modes, 86
  Settings Window, 86
AT&T Managed Services, 11
AT&T Managed VPN Services (AVTS), 76
AT&T Service Manager. *See* AT&T Authentication Server
Authentication, 12
AutoConnect, 39
Automatic Connection, 22
Automatic Prompting, 24
Automatic Updates, 40, 140
  Other programs, 32
Autostart, 30

C

Cellular, 99, 112
Central Configuration. *See* Configuration
Command Line Options, 56
Configuration, 22, 101
  Advanced, 26
  Central, 26
  Login Properties, 26
  Setup Wizard, 24
Connection Sequence, 22
Customizations, 47

D

Default Service, 27
Digital Certificates, 13, 99
Distribution, 18
  MSI, 18
DNS, 28
Domain Suffix, 28
Dynamic DNS, 89

E

Editions, 17
Extended Access, 11, 76

F

Fenced Internet, 88
Firewall Settings, 137
FixedIP, 111
FixedIP Dual Access, 111

H

Help, 98

I

Installation, 17
  Checklist, 16
  Editions. *See* Editions
  Requirements, 15
Installation Log, 100
InstallShield, 17, 47
Internet Explorer Proxy Settings, 33
IPSec, 89
IPSec Encryption, *90*

L

LDAP. *See* Digital Certificates
Lightweight Policy Enforcement, 12, 77, 79
  Threshold, 78
Login Properties. *See* Configuration
LPE. *See* Lightweight Policy Enforcement

M

Managed IPSec Dual Access VPN, 111
Managed IPSec VPN, 111
Managed SSL Dual Access VPN, 111
Managed SSL VPN, 111
Managed VPN IPsec, 89
Managed VPN Services, 11
MaxNumFilters, 20
Microsoft IPSec, *90*
Mobile PC, 34
Multi-Homing

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Preventing, 39

N

NAT Traversal, *90*
Network Firewall Configuration, 137
Network Service
  Default. *See* Default Service

P

Persistent Connections, 34
Points of Presence (PoPs), 11, 76
Preferences, 29
Profile Manager, 27
Profiles, 26
Program Control, 77
Proxy, *91*

R

RADIUS, 13
RAS. *See* Remote Access Service
Remote Access Service, 11
Remove, 43

S

SafeWord, 13
SDK Definitions, 118, 119
SecurID, 13, 25
Sharing Local Resources, 89
SoftToken, 13
Software Updates. *See* Automatic Updates
SSL, *91*
System Requirements. *See* Installation

T

Timeouts, 33
Token, 25prop
Trusted Domain Customization, 61

U

UDP Encapsulation, *90*
Uninstall, 43
Upgrading Client Software, 19

V

VPN Mobility, 34

W

Windows Installer, 18, 47
  Features, 47
  Public Properties, 49
  Shortcuts, 55
  Transform, 57
Windows Logon, 28
WINS, 28

X

x.509, 99

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. Images are shown for illustrative purposes only; individual experience may vary. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.